WYDAWNICTWO SIGMA NOT

ISSN 0542-9951

7
1995

informatyka

Generalny Dostawca Systemów Informatycznych

CSBI

Computer Systems for Business International SA

informatyka

Miesięcznik
ISSN 0542-9951
INDEKS 36124

nr 7 1995
Lipiec
Rok wydania XXXI

Uwaga!
Zmiana adresu
i telefonów redakcji
szczegóły w stopce – obok

W numerze:

Strona

Bezpieczeństwo systemów informatycznych – *Andrzej Bylicki* 1
Koncepcja realizacji poczty elektronicznej X.400 w TP S.A. – *Sławomir Michalski, Marian Suskiewicz* 8
Systemy logistyczne wyzwaniem dla informatyków – *Stefan Abt* 12
Homologacja systemów informatycznych – *Zdzisław Szyjewski* 16
Perspektywy rozwoju rynku komputerów osobistych – *Robert Repeć* 19
Systemy czasu rzeczywistego
Normy IEC dla systemów komputerowych związanych z bezpieczeństwem – *Zdzisław Żurakowski* 22
Mobitex w Warszawie – *Przemysław Baszkiewicz* 29
WebForce – pakiet komercyjnej obsługi WWW (*pb*) 30
3Com – zarządzanie pakietami w środowisku SNA/IBM (*k*) 31
Compaq Presario – więcej niż komputer (*k*) 31
Serwery HP klasy K (*k*) 31

W najbliższych numerach:

- **Waldemar Wieczerzycki i Robert Wrembel prezentują perspektywy w relacyjnych bazach danych.**
- **Katarzyna Lange przedstawia informacje na temat błędów, jakie mogą wystąpić przy transmisji komunikatów EDI.**
- **Marian Kuraś i Linda E. Duxbury charakteryzują problematykę strategicznych zastosowań techniki informacyjnej.**
- **Jan Ryżko opisuje stan elektroniki światowej w roku bieżącym oraz jej perspektywy w latach następnych.**
- **Gerhard Rabe i Günter Glöe omawiają atestację, certyfikację i licencjonowanie systemów komputerowych pełniących funkcje związane z bezpieczeństwem.**

REDAGUJE ZESPÓŁ:
mgr Bogdan **MIŚ**
(redaktor naczelny)
mgr Krystyna
KARWICKA-RYCHLEWICZ
(zastępca redaktora naczelnego)
mgr Teresa **JABŁOŃSKA**
(sekretarz redakcji)
Alina **KLEPACZ**
(sekretariat)

KOLEGIUM REDAKCYJNE:
prof. dr hab. Leonard BOLC,
mgr inż. Piotr FUGLEWICZ,
prof. dr hab. Jan GOLIŃSKI,
dr inż. Zenon KULPA,
doc. dr inż. Jan MULAWKA,
prof. dr hab. Wojciech OLEJNICZAK,
mgr inż. Jan RYŻKO,
dr Witold STANISZKIS,
dr inż. Jacek STOCHLAK,
prof. dr hab. Maciej STOLARSKI,
dr hab. Zdzisław SZYJEWSKI,
prof. dr hab. inż.
Ryszard TADEUSIEWICZ,
prof. dr hab. Jan WĘGLARZ.

PRZEWODNICZĄCY
RADY PROGRAMOWEJ
prof. dr hab.
Juliusz Lech KULIKOWSKI

WYDAWCA:
Wydawnictwo Czasopism i Książek Technicznych SIGMA NOT Spółka z o.o.
ul. Ratuszowa 11
00-950 WARSZAWA
skrytka pocztowa 1004

Redakcja:
01-950 Warszawa,
ul. Ratuszowa 11, p. 628 i 644
skrytka pocztowa 1004
tel., fax: 619-11-61
tel.: 619-22-41 w. 159

Materiałów nie zamówionych redakcja nie zwraca

Autorzy artykułów proszeni są o przysyłanie tekstów na dyskietkach – w czystych kodach ASCII (Latin II, Mazovia) lub edytorach: Word 2, Word 6 – oraz odbitki na papierze.

W sprawach ogłoszeń prosimy zwracać się bezpośrednio do Redakcji lub Działu Reklamy i Marketingu
00-950 Warszawa
ul. Mazowiecka 12
telefon: 27-43-66
telefaks: 26-80-16

Warunki prenumeraty na 1995 r.

Zamówienia na prenumeratę czasopism wydawanych przez Wydawnictwo SIGMA-NOT można składać w dowolnym terminie. Mogą one obejmować dowolny okres czasu, tzn. dotyczyć dowolnej liczby kolejnych zeszytów każdego czasopisma.

Zamawiający może otrzymywać zaprenumerowany przez siebie tytuł począwszy od następnego miesiąca po dokonaniu wpłaty. Zamówienia na zeszyty sprzed daty otrzymania wpłaty będą realizowane w miarę możliwości – z posiadanych zapasów magazynowych.

Warunkiem przyjęcia i realizacji zamówienia jest otrzymanie z banku potwierdzenia dokonania wpłaty przez prenumeratora. Dokument wpłaty jest równoznaczny ze złożeniem zamówienia.

Wpłat na prenumeratę można dokonywać na ogólnie dostępnych blankietach w Urzędach Pocztowych (przekazy pieniężne) lub Bankach (polecenie przelewu), przekazując środki pod adres:
Wydawnictwo SIGMA-NOT Spółka z o.o.
Zakład Kolportażu
00-716 Warszawa, skr. poczt. 1004
konto:
PBK S.A. III 0/Warszawa nr 370015-1573-139-11

Wpłaty na prenumeratę przyjmują także wszystkie urzędy pocztowe nadawczo-odbiorcze oraz doręczyciele na terenie całego kraju

Na blankiecie wpłaty należy czytelnie podać nazwę zamawianego czasopisma, liczbę zamawianych egzemplarzy, okres prenumeraty oraz własny adres.
Na życzenie prenumeratora, zgłoszone np. telefonicznie, Zakład Kolportażu ul. Bartycka 20, 00-950 Warszawa, (telefony: 40-30-86, 40-35-89 oraz 40-00-21 wew. 249, 293, 299) wysyła specjalne blankiety zamówień wraz z aktualną listą tytułów i cennikiem czasopism.

Odbiorcy zagraniczni mogą otrzymywać czasopisma poprzez prenumeratę dewizową (wpłata dokonywana poza granicami Polski w dewizach, wg cennika dewizowego z cenami podanymi w dolarach amerykańskich) lub poprzez zamówioną w kraju prenumeratę ze zleceniem wysyłki za granicę (zamawiający podaje dokładny adres odbiorcy za granicą, dokonując równocześnie wpłaty w wysokości dwukrotnie wyższej niż cena normalnej prenumeraty krajowej).

Egzemplarze archiwalne (sprzedaż przelewowa lub za zaliczeniem pocztowym) można zamawiać pisemnie, kierując zamówienia pod adresem: Wydawnictwo SIGMA NOT, Spółka z o.o. Zakład Kolportażu, 00-716 Warszawa, ul. Bartycka 20, paw. B, tel. 40-37-31, natomiast za gotówkę można je nabyć w Klubie Prasy Technicznej w Warszawie ul. Mazowieckiej 12, tel. 26-80-17.

Istnieje możliwość zaprenumerowania 1 egz. czasopisma po cenie ulgowej przez indywidualnych członków stowarzyszeń naukowo-technicznych zrzeszonych w FSNT oraz przez uczniów zawodowych i studentów szkół wyższych. Blankiet wpłaty na prenumeratę ulgową musi być opatrzony na wszystkich odcinkach pieczęcią koła SNT lub szkoły.

W przypadku zmiany cen w okresie objętym prenumeratą Wydawnictwo zastrzega sobie prawo do wystąpienia o dopłatę różnicy cen oraz prawo do realizowania prenumeraty tylko w pełni opłaconej.
Cena jednego egzemplarza: normalna 4,50 zł (45 000 zł), ulgowa 3,15 zł (31 500 zł)
Wartość prenumeraty w zł:
Normalna: kwartalna 13,50 zł (135 000 zł), półroczna 27 zł (270 000 zł), roczna 54 zł (540 000 zł)
Ulgowa: kwartalna 9,45 zł (94 500 zł), półroczna 18,90 zł (189 000 zł), roczna 37,80 zł (378 000 zł)

Skład i druk: Drukarnia SIGMA NOT Sp. z o.o. z. 200/95

Bezpieczeństwo systemów informatycznych

Andrzej Bylicki
Hewlett-Packard Polska
Warszawa

P. 1877/95

Termin **bezpieczeństwo systemów informatycznych**, definiowany przez Komitet X/Open jako: *...stan systemu IT, w którym poziom ryzyka jego aplikacji jest zredukowany do akceptowalnego poziomu poprzez zastosowanie odpowiednich środków...* obejmuje problematykę bezpieczeństwa zewnętrznego, tj. wpływu systemu (jego funkcjonowania i awarii) na środowisko, w którym działa oraz problematykę bezpieczeństwa wewnętrznego, który to termin z kolei obejmuje trzy klasy zagadnień:

- **dostępność** (ang. *availability*) – rozumiana jako oczekiwany poziom ciągłości dostępności usług i zasobów (danych),
- **integralność** (ang. *integrity*) – gwarancja pewności i zaufania do gromadzonych i przetwarzanych danych – ich oryginalności,
- **poufność** (ang. *confidentiality*) – dostęp do danych (odczyt-zapis) i zasobów sprzętowych powinien być możliwy tylko dla uprawnionych osób (procesów).

Inny podział wyodrębnia bezpieczeństwo logiczne (określony poziom ograniczeń nieuprawnionego dostępu do zasobów systemu) oraz fizyczne, definiowane jako ograniczenie niepożądanego fizycznego dostępu do systemu.

Spotkać można także jeszcze inny podział pojęcia „bezpieczeństwo systemów komputerowych":

- bezpieczeństwo bierne – szyfrowanie, kopie bezpieczeństwa,
- bezpieczeństwo aktywne – ograniczanie dostępu, identyfikacja, kontrola uprawnień itp.

Zagadnienia bezpieczeństwa obejmują też stosunkowo nowy obszar związany z upowszechnianiem się komputerowo realizowanych przesłań (dokumentów – EDI, środków pieniężnych – SWIFT itp.) – **niezaprzeczalność** (ang. *non-repudiation*) wysłania i odbioru.

Niniejszy artykuł koncentruje się na szczegółowym przedstawieniu rozwiązań gwarantujących logiczne bezpieczeństwo wewnętrzne unixowych systemów komputerowych.

Dostępność

Jednym z najkosztowniejszych składników intensywnie eksploatowanego systemu komputerowego są zgromadzone w nim dane. Najistotniejszym więc działaniem jest zapewnienie ich pełnej dostępności dla użytkowników, niezależnie od działań i zdarzeń zewnętrznych czy wewnętrznych. Według szczegółowych badań prowadzonych przez *Contigency Planning Research*, a opublikowanych w czasopiśmie „Operation and Fulfillment" nr 5–6, 1994, najczęstszą przyczyną utraty danych są awarie zasilania (45,3%), wydarzenia losowe (29,8%) oraz uszkodzenia: sprzętu (6,7%), sieci (3,2%) i oprogramowania (1,5%). Negatywne skutki zadziałania dowolnej z ww. przyczyn mogą być co najmniej minimalizowane przez zastosowanie odpowiednich zabezpieczeń.

Ochrona przed zanikiem zasilania:

- zasilacze nieprzerywalne (UPS),
- baterijne podtrzymanie jednostki centralnej (*battery back-up unit*),

Ochrona przed awarią podsystemu dyskowego:

- macierze dyskowe (RAID – *Random Array of Inexpensive*/Independant Disk) – zespoły dysków pracujące w konfiguracjach gwarantujących bezzwłoczną, niezauważalną dla użytkownika, likwidację awarii jednego lub kilku dysków (patrz tab. 1);
- inną (kosztowną) metodą podwyższania niezawodności podsystemu dyskowego jest pełne dublowanie (ang. *duplexing*) wszystkich jego składników.

Ochrona przed utratą zgromadzonych danych.

Tworzenie kopii bezpieczeństwa (ang. *back-up*) jest powszechnie stosowaną metodą zwłocznego zapewnienia dostępności danych w przypadku, gdy dane bieżące (on-line – najczęściej pamiętane na dyskach) z jakiegokolwiek powodu uległy zniszczeniu lub zostały utracone. Jest to szybka, a także tania technika zapewnienia prawie nieprzerwanej ciągłości dostępu do danych w porównaniu do kosztu czasu ich „ręcznego" odtwarzania, które wg NCSA wynoszą dla 1 MB od ok. 800 USD 1 dzień dla danych finansowych do ok. 5000 USD/2 dni dla danych inżynierskich i naukowych.

W poniższych rozważaniach celowo pominięto tak jeszcze do niedawna popularną archiwizację na dyskietkach (ang. *stackup*). Uczyniono tak, gdyż przy obecnych pojemnościach dysków czy nawet pojedynczych zbiorów (od kilkuset MB do kilkuset GB dla rzeczywistych zastosowań komercyjnych) jest to rozwiązanie o bardzo niskiej funkcjonalności i znacznym, relatywnie do innych technik, np. QIC czy DAT, koszcie bezpośrednim (powyżej 0,5 $ za 1 MB) oraz znacznych kosztach pośrednich (dużo większy niż przy innych technikach nakład pracy).

Podstawowymi kryteriami doboru metody archiwizacji są: koszt przechowywania, czas zapisu i odzyskiwania danych oraz trwałość zapisu.

Najczęściej obecnie stosowanymi urządzeniami archiwizującymi, pracującymi pojedynczo lub w zespołach (w tym z automatycznymi zmieniaczami) są tzw. biblioteki (ang. *juke-box*), a dołączane do systemu komputerowego przez jeden ze standardowych interfejsów (SCSI, Fibre Link, Fast/Wide/Differential SCSI), są następujące typy nośników:

- Taśmy 1/2 cala
  Podstawowe typy: PE (*Phase Encoding*) – 1600 cpi, GCR – 6250 cpi.
  Typowe pojemności jednej taśmy 2400 m: PE – 40 MB; GCR – 140 do 700 MB (z kompresją).
  Maksymalna szybkość transferu: od 0,2 (PE) do 1 MBps.
  Średni czas dostępu: kilka minut.
  Koszt przechowywania 1 MB: ok. 0,1 USD.
  Trwałość: od 5 do 20 lat.

- Taśmy QIC (*Quarter Inch Cartridge*) – 1/4 cala
  Normy – formaty zapisu QIC:
  QIC-24 – 60 MB
  QIC-40 – 40 MB
  QIC-80 – 80 MB
  QIC-120 – 125 MB
  QIC-150 – 150 MB
  QIC-525 – 525 MB
  QIC-1000 – 1 GB
  QIC-1350 – 1,35 GB
  QIC-3010 i 3020 – napędy z głowicami magneto-opornościowymi o podwyższonej pojemności
  QIC-122 i 123 – format danych skompresowanych i algorytmy kompresji
  QIC-02, 36, 104 i 121 – interfejsy dla urządzeń QIC.
  Normy dotyczące nośników dla urządzeń standardu QIC:
  – DC6000 – duża kaseta
  – DC2000 – mała kaseta
  – DC9135 – taśma o lepszych parametrach i o rozmiarach, jak DC6000 oraz ich wersje: DC6150, DC2120.
  Maksymalna szybkość transferu: ok. 0,6 MBps.
  Średni czas dostępu: 30–40 s.
  Koszt – przechowywania 1 MB: od 0,2 do 0,5 USD,
  – nośnika dla 1 MB: 0,1 USD.
  Czas archiwowania 1 GB: ok. 70 min.
  Trwałość: od 5 do 20 lat.

- Taśmy DAT (*Digital Audio Tape*) – 4 mm
  DDS (*Digital Data Storage*) – format zapisu danych,
  DDS-DC – rozszerzenie DDS realizujące DCLZ,
  Typowe pojemności jednej taśmy (kasety): 2–8 GB (po kompresji).
  Czas zapisu-odczytu 1 GB: ok. 0,5 godz.
  Maksymalna szybkość transferu: od 0,183 do 0,732 MBps.
  Średni czas dostępu: 25 s.
  Koszt – przechowywania 1 MB: ok. 0,1 USD,
  – nośnika dla 1 MB: ok. 0,02 USD.
  Czas archiwowania 1 GB: ok. 1,5 godz.
  Trwałość: od 5 do 20 lat.

- Taśmy 8 mm (jedyny wytwórca: Exabyte)
  Formaty danych: EXB-8500.
  Typowe pojemności jednej taśmy (kasety): 5–10 GB (po kompresji).
  Maksymalna szybkość transferu: od 0,5 do 1 MBps.
  Średni czas dostępu: kilka minut (ok. 2).
  Koszt – przechowywania 1 MB: ok. 0,1 USD,
  – nośnika dla 1 MB: <0,004 USD.
  Czas archiwowania 1 GB: ok. 40 min.
  Trwałość: od 5 do 20 lat.

- Taśmy DLT – wytwarzane przez jednego wytwórcę; kosztowne, ale bardzo szybkie i pojemne.

- Dyski optyczne jednokrotnego zapisu – WORM (*Write Once Read Many*)
  Pojemność jednego dysku: do 2 GB.
  Średni czas dostępu: 0,15 s.
  Koszt – przechowywania 1 MB: ok. 0,5 USD.
  – nośnika dla 1 MB: ok. 0,1 USD.
  Czas archiwowania: 1 GB – ok. 40 min.
  Trwałość: pow. 10 lat.

- Dyski magnetooptyczne wielokrotnego zapisu (MO)
  Pojemność jednego dysku: do 2 GB.
  Średni czas dostępu: mniej niż 0,05 s.
  Koszt – przechowywania 1 MB: od ok. 0,5 USD (biblioteki) do ok. 4 USD (pojedyncze).
  – nośnika dla 1 MB: 0,1 USD.
  Czas archiwowania 1 GB – ok. 40 min.
  Trwałość: pow. 10 lat.

- Archiwizery typu IBM 3480
  Pojemność 1 taśmy: do 4 GB.
  Średni czas dostępu: 15 s.
  Koszt – przechowywania 1 MB: ok. 0,5 USD.
  – nośnika dla 1 MB: ok. 0,03 USD.
  Czas archiwowania 1 GB: ok. 10 min.
  Trwałość: pow. 10 lat.

Pojemność nośników jest zwiększana (nawet czterokrotnie) przez stosowanie różnych metod kompresji:
– LZ – *Lempel Ziv*,
– LZW – *Lempel Ziv Welch*.
Szybkość dostępu do danych jest zwiększana za pomocą techniki QFA (*Quick File Access*).
Technikę tę stosuje większość systemów DAT i Exabyte.

Tabela 1. Klasyfikacja i cechy różnych typów macierzy dyskowych

Typ	Nazwa (opis)	Koszt*) relatywny	Dostępność*) MTBF	Wydajność	
				Odczyt	Zapis
0/DSA	Jednoczesny zapis-odczyt na wielu dyskach – przeplot (ang. data striping)	M	1	>1	>1
1/MDA	Dyski lustrzane – zapis równoległy na dysku zasadniczym i rezerwowym	2M	2M	1	<1
2	Przeplot bitowy z kodem korekcyjnym Hamminga. Niski współczynnik „cena do wydajności"				
3/PDA	Przeplot bitowo-bajtowy z wydzielonym dyskiem do zapisu kodów korekcyjnych parzystości	M+1	<2M	1	1
				operacje sekwencyjne, duże bloki danych	
				≪1	≪1
				operacje swobodne, małe bloki danych	
4/IDA	Przeplot sektorów (bloków). Dodatkowy dysk dla kodów korekcyjnych parzystości	M+1	<2M	<1	≪1
5	Przeplot blokowy. Bez wydzielonego dysku dla kodu korekcji błędów	M+1	<2M	>1	≪1
6	Jak w typie 0, z tym, że poszczególne bloki są dodatkowo kopiowane na inny dysk	2M	2M	>1	<1
10 1/0	Kombinacja typów 0 i 1. Wielodyskowe zestawy – zasadniczy i rezerwowy – umożliwiające równoczesne operacje wielodyskowe (ang. data striping)	2M	2M	>1	1

*) w relacji do prostego zestawu M dysków (JBOD – *Just Bunch Of Disks*) i dużego pojedynczego dysku (SLED – *Single Large Expensive Disk*) o tej samej pojemności, dla których wartości ww. parametrów są odpowiednio równe: koszt: M i $n*M$ ($0 < n < 1$); dostępność: 1 i M; wydajność: 1 i 1;
DSA – *Data Striping without parity Array* PDA – *Parallel Disk Array*
MDA – *Mirrored Disk Array* IDA – *Independant Disk Array*

Biblioteki taśmowe (8 mm) i MO osiągają pojemności do kilkuset GB. Przez odpowiednie oprogramowanie (np. Amass) mogą być one widziane przez użytkowników jako nieco wolniejsza część dyskowego systemu plików.

Interesującym rozwiązaniem jest stosunkowo niedawno wprowadzony przez firmę HP, kompleksowy, w pełni zautomatyzowany zestaw archiwizujący. (Obejmuje on urządzenia z automatycznymi zmieniaczami nośników oraz inteligentne oprogramowanie obsługujące wszystkie aspekty pełnego procesu archiwizacji). Zestaw ten o nazwie LABS (*Low Admin Backup for Servers*) praktycznie eliminuje konieczność angażowania się administratora w proces archiwizacji.

Strategia archiwizacji

Istotny jest wybór metody dokonywania archiwizacji i gospodarki nośnikami. Powinna ona zapewnić wysoki stopień ochrony danych przy minimalnym koszcie i liczbie używanych nośników. Najgorszą metodą jest używanie do archiwizowania ciągle jednego nośnika. W tym przypadku wykrycie błędu po dokonaniu archiwizacji pozbawia możliwości sięgnięcia do poprzedniej – poprawnej – wersji.

Lepszą jest metoda dwunośnikowa, polegająca na naprzemiennym wykonywaniu kopii pełnych lub częściowych. Znacznie lepszą jest metoda trójnośnikowa o cyklu tygodniowym:

- pełna archiwizacja w pierwszym dniu na nośniku nr 1,
- przyrostowe archiwizacje w dniach 2, 3, 4 i 5 (+6) na nośniku nr 2; pełna archiwizacja na nośniku nr 3, a nośnik nr 1 jest przenoszony do archiwum zewnętrznego. Nośnik nr 2 jest wykorzystywany do archiwizacji przyrostowych w kolejnych dniach itd. Po 2 tygodniach nośnik nr 1 wraca i na nim jest dokonywana kolejna pełna archiwizacja. Metoda ta jest zalecana przy małych zmianach dziennych.

Modyfikacją metody trójnośnikowej jest metoda z użyciem 6(7) nośników, różniąca się od poprzednio omówionej stosowaniem odrębnych nośników dla kolejnych archiwizacji przyrostowych. Jest ona zalecana przy znacznych zmianach dziennych danych.

Metoda z 10 nośnikami obejmuje sześcionośnikową + trzy nośniki z archiwum pełnym tygodniowym oraz jeden dodatkowy nośnik dla pełnego miesiąca.

Inne stosowane metody archiwizacji, to:

- 3 × 5 nośników (3-tygodniowe): w każdym tygodniu cztery archiwa przyrostowe (w kolejne dni) oraz jedno pełne w dniu piątym;
- 22-nośnikowe (roczne): 5 nośników dla każdego dnia tygodnia, 5 nośników dla pełnych archiwów kolejnych tygodni (wykonywanych wraz z archiwizacją w dniu 5) oraz 12 dla archiwów miesięcznych wykonywanych w ostatni dzień miesiąca.

Pamiętać jednak należy, że:

- nośniki, a szczególnie taśmy, zużywają się i dlatego zawsze trzeba mieć w zapasie przynajmniej jeden nie używany,
- napędy powinny być okresowo czyszczone (np. co 20 zapisów-odczytów),
- po każdej archiwizacji powinna być dokonywana operacja porównania zawartości archiwum z zawartością oryginalną,
- szczególnej ochronie powinny podlegać archiwa zewnętrzne,
- w sytuacjach, gdy koniecznym jest zapewnienie wysokiego stopnia wierności i niezmienności danych archiwalnych (w tym niepodleganie modyfikacjom), stosowaną techniką powinny być napędy i nośniki WORM.

Archiwa wielopoziomowe

Użytkowanie i zarządzanie wielopoziomowymi, niejednorodnymi podsystemami pamięci zewnętrznych umożliwiają narzędzia HSM (*Hierarchical Storage Management*). Są to zestawy środków sprzętowych i programowych umożliwiających archiwowanie i odzyskiwanie danych z hierarchicznie usystematyzowanych archiwów. Podstawowym kryterium umieszczenia danych na odpowiednim poziomie hierarchii jest częstość ich używania.

W systemach HSM określone są cztery zasadnicze obszary funkcjonalne:

- Pamięć pierwotna, realizowana zwykle na dyskach magnetycznych;
- Archiwum pierwotne – dyski, taśmy lub nośniki optyczne (magneto-optyczne),
- Archiwum wtórne „płytkie" – zbiory usunięte z pamięci pierwotnej, oczekujące na przeniesienie do archiwum wtórnego „głębokiego", realizowane zwykle na dyskach magnetycznych lub magnetooptycznych (kryterium: stosunkowo krótki czas dostępu);
- Archiwum wtórne „głębokie" – właściwe archiwum długoterminowe, realizowane zwykle na nośnikach taśmowych (kryterium: niski koszt przechowywania),

Wyróżnia się następujące poziomy HSM:

0 – automatyczna archiwacja, ręczne odzyskiwanie;
1 – automatyczne, transparentne archiwowanie i odzyskiwanie;
2 – jak poziom 1 plus indywidualnie przydzielane ograniczenia – poziomy zapełnienia dysków (ang. *watermarks*), których osiągnięcie powoduje automatyczne rozpoczęcie lub zakończenie operacji archiwowania,
3 – poziom 2 uzupełniony o zarządzanie warstwami hierarchicznego systemu pamięciowego; poziom ten zawiera: dynamiczne monitorowanie warstw i zarządzanie nimi, zarządzenie woluminami, kolejkowanie zadań oraz optymalizowanie wydajności;
4 – jak poziom 3 plus klasyfikacja i reguły przetwarzania zbiorów;
5 – poziom 4 wzbogacony o zarządzanie obiektami i ustrukturalizowanymi lub nie zapisami umożliwiającymi ich użycie przez DBMS.

Produkty realizujące HMS oraz ich producentów zawiera tab. 2.

Rozważając zastosowanie archiwum wielopoziomowego i narzędzi HMS należy każdorazowo przeprowadzić dokładną analizę kosztów dwu wariantów: HSM i archiwum na dyskach, gdyż ze względu na ciągły naprzemienny ruch cen w dół składników obu rozwiązań, prostszy i sprawniejszy system z archiwum jednorodnym na dyskach magnetycznych może okazać się tańszy.

Ochrona przed uszkodzeniem jednostki centralnej

Stosowane są następujące konfiguracje zapewniające podwyższoną dostępność jednostek centralnych:

- z systemem rezerwowym, automatycznie przejmującym obsługę funkcji systemu głównego (np. Switch-Over – HP, HACMP – IBM, Fusion – SUN, LifeKeeper – NCR);
- grona (ang. *cluster*) – o czasach przejmowania funkcji uszkodzonego systemu od kilkuset (*cold*) do kilkudziesięciu (*warm/hot*) sekund.

Znaczną redukcję czasu przejmowania w systemach unixowych uzyskuje się przez stosowanie w systemie operacyjnym funkcji dziennikującej (ang. *journalling* – systemu plików JFS) i wyeliminowanie czasochłonnej funkcji *fsck*.

Ochrona przed niesprawnością sieci komputerowej

Realizowana jest najczęściej przez duplikowanie połączeń lub tworzenie takiej topologii, że z dowolnego do innego dowolnego punktu istnieje w sieci więcej niż jedna droga przesyłania.

Integralność

Integralność to wierność – zgodność z oryginałem implikująca zaufanie do zgromadzanych danych. Jest silnie zależna od metod ich gromadzenia i przechowywania oraz jakości oprogramowania, a także od poziomu ochrony przed nieuprawnionym wprowadzaniem i modyfikowaniem danych (dostępem do nich). Stwierdzeniu wierności i niezaprzeczalności służą techniki MAC (*Message Authentification Code*) i podpisu cyfrowego (ang. *digital signature*).

Identyfikacja użytkownika (ang. *authentication*) oraz określenie jego uprawnień do dysponowania określonymi zasobami i do dokonywania dostępnych jemu operacji (ang. *authorization*) jest zwykle dokonywana przez mechanizmy zawarte w systemie operacyjnym.

Poziom zabezpieczeń (wbudowanych mechanizmów) systemu operacyjnego jest określany przez spełnianie zestawu następujących kryteriów:

- TCSEC (*Trusted Computer Security Evaluation Criteria*) – tzw. Pomarańczowa Księga – jest zestawem kryteriów określonych w USA przez NTSC (*National Computer Security Center*) dla systemów użytkowanych w sektorach: rządowym, militarnym itp. W Europie opracowano zestaw podobnych kryteriów określanych akronimem ITSEC (*Information Technology Security Evaluation Criteria*).
  W obu tych zestawach wyróżnia się następujące, prawie dokładnie odpowiadające sobie poziomy bezpieczeństwa (uszeregowane od najniższego do najwyższego):
  - w TCSEC – *D*, *C*1, *C*2, *B*1, *B*2, *B*3, *A*1
    D – minimalny poziom zabezpieczeń,
    Cn – zabezpieczenia uznaniowe,
    Bn – zabezpieczenia obligatoryjne,
    *A*1 – zweryfikowane bezpieczeństwo;
  - w ITSEC – *E*1, *E*2, *E*3, *E*4, *E*5, *E*6 (kryteria poprawności zabezpieczeń);
  - *F-C*1, *F-C*1, *F-B*1, *F-B*2, *F-B*3 (kryteria funkcjonalne).
- MSFR (*Minimum Security Functionality Requirements*) dla systemów komercyjnych, w których nacisk położono na nieco inne cechy, np. identyfikacja nadawcy i odbiorcy, niezaprzeczalność nadania i odbioru itd.
- ANSI/ISO normy dla sektora bankowego. (*X*3.*x*, *X*9.*x*/8372, 8730, 8731, 11131, 10126).
  I tak np. system operacyjny HP-UX (Hewlett-Packard Unix) może być dostarczony w dwu różnych z punktu widzenia bezpieczeństwa wersjach:
  - **standardowej** o poziomie bezpieczeństwa *C*2 (identyfikacja użytkownika, zapis aktywności (auditing), uznaniowa kontrola dostępu DAC (*Discretionary Access Control*), izolacja procesów, niszczenie śladów obiektów używanych przez poprzednio realizowane procesy);
  - **BLS** (*B-Level Security*) – o podwyższonym poziomie do *B*1 z elementami *B*2, spełniającej kryteria poziomu *C*2 i uzupełnionej o: listy kontroli dostępu ACL (*Access Control Lists*), obligatoryjną kontrolę dostępu MAC (*Mandatory Access Control*), etykietowanie przedmiotowe i podmiotowe (*sensitivity labels*), rozdzielenie funkcji superadministratora na trzech administratorów wydzielonych obszarów funkcjonalnych (użytkownicy, audytowanie, funkcje systemowe), definicję dopuszczalnych okresów dostępu dla użytkowników ATOD (*Application Time Of Day*); zabezpieczonych (zaszyfrowanych i wyłączonych z powszechnego dostępu) baz danych identyfikacyjnych; zaufaną ścieżkę (*trusted path*), zapobiegającą przechwyceniu danych identyfikacyjnych podczas procesu identyfikacji w celu późniejszego ich użycia do uzyskania dostępu (ang. *masquerading*, *spoofing* i inne). Wersja ta spełnia wymogi CMW.

Obecnie trwają prace nad wersją w pełni spełniającą kryteria poziomu *B*2. Identyczne poziomy bezpieczeństwa realizują nowsze wersje IBM-owskiego systemu AIX.

Poziom bezpieczeństwa sieci komputerowej jest definiowany na podstawie spełniania kryteriów zawartych w TNI (*Trusted Networking Interpretation*), tzw. *Czerwonej Księdze* oraz norm MAXSIX (*Multi-vendor trusted networking*), uzgodnionych przez czołowych dostawców produktów sieciowych. W miarę kompleksowe zasady

Tabela 2. Produkty realizujące HMS oraz ich producenci

Poziom	Produkt	Producent
0	Arcserve-Roslyn	Cheyenne Software Inc.
	Migtool	Delta Microsystems
	DECnsr	Digital Equipment Corp.
	Networker HSM	Legato Systems Inc.
	Alexandria-Boulder	Spectra Logic
	OpenView OmniBack II	Hewlett Packard
1	Netarchive	Advanced Software Concepts
	Emissary/HSM	Alphatronix Inc.
	Archivist	Netstor
	OpenV*Migrator	OpenVision
2	Unicenter	CA International Inc.
	Sparcus	Hiarc
	Palindrome HSM	Palindrome Technologies
	MastarMind	Qstar
	OpenView OmniStorage	Hewlett Packard
3	Conner HSM	Conner
	Open Storage Manager	Lachman Technology Inc.
	OpenV*HSM	Openvision
	Hierarchy	Software Partners/32
4	Firetrek-Carlsbad	Artecon Inc.
	Epochserve Suite	Epoch Systems Inc.
nieokreślony	AMASS	Advanced Archival Products Inc.
	Datamigrator	AT & T Commvault Systems
	Computer upgrade HSM	Computer Upgrade Corp.
	Polycenter HSM	Digital Equipment Corp.
	Epochmigration	Epoch System Inc.
	FileServ	E-System Inc.
	Flextor HSM	Introl Corp.
	Storage Center	Software Partners/32
	Nearnet	Storage Technology Corp.

zarządzania hasłami zawarte są w PMG (*Password Management Book*) – tzw. *Zielonej Księdze* opracowanej przez Departament Obrony USA.

Istotny dla bezpieczeństwa procesu identyfikacji jest zwykle dwufazowy („identyfikator", np. login i jego utajnione potwierdzenie, np. hasło) i może być dokonywany wg dowolnej z czterech metod:

- na podstawie zasobu wiedzy użytkownika: faktów i danych znanych w zasadzie tylko jemu, np. danych osobistych użytkownika czy jego bliskich, indywidualnego, tajnego hasła (ang. *something they know*). Metoda ta jest jednak mało bezpieczna;
- na podstawie posiadanych przez użytkownika przedmiotów-identyfikatorów: żetonów (ang. *token*), kart magnetycznych (ang. *something they have*);
- na podstawie posiadanych identyfikatorów fizycznych: kart inteligentnych (ang. *smart card*), identyfikatorów aktywnych (ang. *active-badge*) i związanych z nimi identyfikatorów logicznych: haseł, numeru PIN – *Personal Identification Number* (ang. *something they have and they know*);
- na podstawie cech osobniczych (ang. *biometric authentication*): odcisków palców lub dłoni (ang. *finger/hand prints*), charakterystycznych cech głosu (ang. *voice recognition*), oczu (ang. *retinal pattern*) czy podpisu (*signature authentication*) – (ang. *something they are*).

Poufność

Powszechną metodą zachowania poufności przechowywanych lub przekazywanych (przesyłanych) danych jest ich szyfrowanie. Szczególnie istotne jest stosowanie szyfrowania przy przechowywaniu danych poufnych w archiwach zewnętrznych czy przesyłania tego typu danych za pośrednictwem sieci publicznych, np. Internetu.

Na rynku nabywca ma do wyboru produkty realizujące funkcje kryptograficzne bądź sprzętowo, bądź programowo, z zastosowaniem różnego rodzaju algorytmów:

- symetrycznych (np. DES – *Data Encryption Standard*/DEA – *Data Encryption Algorithm* – ISO czy RC2 lub RC4),
- asymetrycznych (np. RSA – *Rivest, Shamir, Adleman*; DSS; *Fiat-Shamir*; MD2, MD4), w których współistnieją dwa klucze: publiczny i prywatny. Publiczny klucz odbiorcy jest używany do zaszyfrowania kierowanych do niego przesłań; klucz prywatny (tajny) służy do ich odszyfrowania. Tylko posiadacz tego klucza może dokonać deszyfracji;
  DSS (*Digital Signature Standard*) – standard podpisu elektronicznego opracowany przez NSA na użytek rządu USA zawiera w sobie algorytm SHA (*Secure Hash Algorithm*);
- posiadających zewnętrzny mechanizm deszyfracji, np. *Skipjack* (technologia *Clipper* – NSA) i *Capstone*, ułatwiających organom rządowym deszyfrację w celu śledzenia i monitorowania przepływu informacji;
- Al Gamal – wymieniany jako algorytm kryptograficzny – składnik normy ANSI X9.31, standaryzującej zagadnienia związane z podpisem elektronicznym;
- FEAL – *Fast Encryption Algorithm* – szybki algorytm szyfrujący, operujący 64-bitowym kluczem (NTT Communication and Information Processing Labs);
- algorytm *Enigma* zgodny z algorytmem stosowanym w maszynach szyfrujących używanych w czasie II wojny światowej. Zaimplementowano go np. w unixowej komendzie (*'crypt' 'ed'* lub *'vi'* z opcją $-x$) w wersji 256-elementowej, ale nie jest zbyt bezpieczny; Istnieją powszechnie dostępne narzędzia (*Crypt Breaker's Workbench*), umożliwiające jego złamanie w dość krótkim czasie (np. dla klucza trzech małych znaków czas ten wynosi ok. 5 min. pracy prostej stacji roboczej).

Dystrybucja algorytmów DES (szczególnie z dłuższymi kluczami – pow. 40 bitów) i RSA poza USA jest silnie ograniczona. Należy zauważyć, że skrócenie, nawet pozornie niewielkie, długości klucza odbija się bardzo mocno na bezpieczeństwie obliczeniowym algorytmu, określanym czasem koniecznym do złamania szyfru. W przypadku kluczy 40-bitowych potrzeba ok. 5 godzin pracy wcale nie najsilniejszej stacji roboczej, by dokonać deszyfracji.

Z kolei Clipper wywołuje ze względu na swoją podstawową cechę (klucz „do drzwi kuchennych"), jaką jest możliwość zdeszyfrowania bez znajomości klucza, powoduje duży opór przyszłych użytkowników w USA, a zwłaszcza tych spoza USA (agendy rządu USA będą dysponentami tej technologii deszyfracji).

Ograniczeniom dystrybucji nie podlegają PGP (*Pretty Good Privacy*), dostępny w sieci Internet oraz PC-IRIS, dostępny poprzez sieć ZiffNet – ogólnie dostępne (*public domian*) systemy kryptograficzne stosujące algorytm RSA z kluczem publicznym, co gwarantuje uproszczenie dystrybucji kluczy. PGP jest wysoko oceniany i popularny wśród użytkowników sieci Internet. Komercyjna wersja PGP jest znana pod nazwą ViaCrypt.

Algorytm DES operuje zwykle kluczem 56-bitowym (poza USA – 40-bitowym) i zapewnia znaczne tzw. bezpieczeństwo obliczeniowe – czas złamania szacuje się na 1000 lat pracy superkomputera Cray2. Szybkość szyfrowania–deszyfrowania jest ok. 15–100 razy większa niż dla algorytmu RSA. Do jego wad trzeba zaliczyć trudne generowanie podpisu elektronicznego i problemy z dystrybucją kluczy. Ostatnio pojawiła się ulepszona wersja tego algorytmu o nazwie *Triple* DES.

W algorytmie RSA stosuje się klucze 512-bitowe. Ma bardzo duże bezpieczeństwo obliczeniowe – 90000 lat na Cray2. Jego podstawowa wada, to mała szybkość szyfrowania–deszyfrowania w porównaniu do innych algorytmów. Umożliwia prostą realizację podpisu elektronicznego, niezaprzeczalności i integralności przesłania (MAC), a także, wynikającą z samej idei tego algorytmu, dystrybucję kluczy i zarządzanie nimi.

Realizacje sprzętowe algorytmów kryptograficznych są znacznie szybsze niż programowe i tylko one mogą być praktycznie stosowane wtedy, gdy wymagane jest dokonywanie szyfrowania–deszyfrowania „w locie". I tak, na przykład, dla DES szybkość szyfrowania przy użyciu układu VLSI wynosi ok. 190 Mbit/s, a dla programu w języku asemblera – 0,84 Mbit/s. Dla RSA odpowiednie liczby wynoszą: 40 Kbit/s i 1 Kbit/s.

Przykładowym rozwiązaniem jest dostarczana przez firmę Hewlett-Packard sprzętowa realizacja modułu kryptograficznego w postaci standardowej karty rozszerzenia HP o następujących cechach:

- pełne zabezpieczenie przed monitorowaniem sygnałów, analizą wewnętrzną i jej przemieszczaniem,
- wbudowany algorytm DES – szybkość szyfrowania 2 Mbit/s,
- procesor sygnałowy (DSP) dla realizacji własnych algorytmów użytkownika, co po uwzględnieniu faktu ograniczeń w dystrybucji algorytmów DES i RSA wydaje się być cechą pożądaną,
- możliwość dołączenia czytnika kart inteligentnych dla identyfikacji użytkownika i przechowywania kluczy,

- oprogramowanie wpisywane przez użytkownika,
- interfejs programowy – API.

Problemy związane z przesyłaniem poufnych informacji między użytkownikami pochodzącymi z różnych systemów (organizacji), tj. unifikację algorytmów i dystrybucję kluczy rozwiązać ma nowo tworzony (przez RSA *Data Security Inc.*) standard PKCS (*Public Key Cryptography Standards*). Stanowi on rozwinięcie PEM (*Privacy Enhanced Mail*). W standardzie PEM dostępne będą dwa tryby pracy – symetryczny i asymetryczny oraz dwa rodzaje kluczy – DEK (*Data Encryption Key*), będący zawsze kluczem systemu DES oraz IK (*Interchange Key*).

Tryby PEM:

- symetryczny – realizujący za pomocą algorytmu DES funkcje: poufność, integralność (generowanie i porównanie MIC (*Message Integrity Check*) – odpowiednika MAC), uwierzytelnianie; IK jest kluczem stosowanego w tym trybie algorytmu szyfrowania;
- asymetryczny – różniący się od symetrycznego realizacją funkcji niezaprzeczalności; W trybie tym będą stosowane algorytmy DES i RSA. IK jest parą kluczy kryptosystemu RSA.

W produktach zarządzania systemami, takich jak *Unicenter* (*Computer Associates*) czy *Tivoli Management Systems*, zawarto rozbudowane rozwiązania zarządzania i kontroli bezpieczeństwa.

Wszystkie wyżej wymienione produkty umożliwiają znaczne podniesienie poziomu bezpieczeństwa węzła sieci komputerowej oraz przechowywanych i przesyłanych danych. Jednak w sieciach rozproszonych występują daleko większe zagrożenia i dlatego konieczne są dodatkowe, dużo bardziej złożone mechanizmy zabezpieczeń, takie jak *Kerberos, Raxco Security Toolkit, RACF*, X.509, *CA Unicenter Security, SecureMax* (*Demax*), *Fortress* (*Los Altos Technology*), *Network/Security Manager* (*Logicon Ultra*) itp.

Bezpieczeństwo w systemach rozproszonych

DCE (*Distributed Computing Environment*) jest to kompleksowy zestaw niezależnych sieciowo usług systemu operacyjnego umożliwiających tworzenie, realizację i konserwację aplikacji rozproszonych (OSF).

Składniki: wątki (ang. threads), RPC – zdalna realizacja procedur, usługi lokalizacyjne (DDS), usługi synchronizacyjne (DTS – *Distributed Time Service*), usługi zabezpieczające (*Distributed Security Service*), DFS (*Distributed File System*) – rozproszony system plików oraz systemy bezdyskowe (ang. *diskless support*).

DDS (*Distributed Directory Services*):

- CDS (Cell DS) – słownik lokalizacji dla pojedynczej komórki (komputerów traktowanych jako wyodrębniony, niepodzielny składnik sieci),
- GDS (Global DS) – globalny słownik lokalizacji zrealizowany z wykorzystaniem standardu X.500,
- XDS (X/Open DS) – X/Open API dla usług lokalizacyjnych,
- GDA (Global Directory Agent) – łączy domeny (obszary) DCE z innymi (administracyjnie) obszarami wykorzystujący X.500 i DNS.

DFS zbudowano z wykorzystaniem mechanizmów zawartych w AFS (*Andrew File System*) – systemu plików stworzonego na Uniwersytecie Cornegie Mellon.

NFS (*Network File System*) – system plików współdzielonych dla sieci TCP/IP – nie zapewnia ani właściwego poziomu integralności, ani bezpieczeństwa i dlatego czasem akronim ten jest odczytywany jako *„No File Security"* – żadnego bezpieczeństwa plików.

DFS/AFS pozwalają na łatwy dostęp do sieci WAN.

W systemach DCE jest stosowany system identyfikacji *Kerberos* wyprowadzony z wersji opracowanej w MIT w ramach projektu Athena, jednak obecnie dość znacznie różniący się od wersji oryginalnej (np. wersja DCE używa RPC – wersja 5 MIT – nie). Kerberos jest silnie wspierany przez OCSG (*Open Computing Security Group*). W systemie Kerberos identyfikacja użytkownika i zezwolenie na użytkowanie określonego serwera sieci w ściśle zdefiniowanym czasie – sesji – następuje przez tzw. bilet (ang. *ticket*), zaszyfrowaną wiadomość składającą się z nazw użytkownika, serwera, adresu sieciowego użytkownika, znacznika czasu i klucza sesji.

W systemie wyróżnia się co najmniej dwa wyodrębnione, dedykowane serwery:

- KAS (*Kerberos Authentication Server*) – serwer identyfikacyjny Kerberosa,
- TGS (*Ticket Granting Server* – serwer (serwery) przydziału biletów, dostępne po uzyskaniu z KAS specjalnego biletu TGT (*Ticket-Granting Ticket*).

Trwają intensywne prace nad normalizacją interfejsu programowego dla zagadnień bezpieczeństwa – GSSAPI (*Generic Security Service API*).

Innym rozwiązaniem zagadnienia identyfikacji w sieciach rozległych jest użycie mostu identyfikującego (ang. *authentication bridge*), do którego są kierowane wszystkie żądania z zewnątrz uzyskania połączenia, i który w przypadku pozytywnej identyfikacji „poleca" właściwemu mostowi komunikacyjnemu zrealizować połączenie.

Wzrost poziomu bezpieczeństwa i uproszczenie procedury metod zabezpieczeń w sieciach TCP/IP są oczekiwane po wprowadzeniu nowych wersji protokołu IP: *IPng* i *IPv4*.

Filtracja przesłań

Powszechną metodą filtrowania (kontroli) dostępu do komputerów pracujących w sieciach jest instalowanie „kurtyn ogniowych" (ang. *firewall*), tj. sprzętu–bramy (ang. *gateway*) oraz oprogramowania filtrującego i rejestrującego ruch do (z) strzeżonych fragmentów sieci.

Dość znanymi przykładami produktów z tego obszaru funkcjonalnego są:

- oprogramowanie instalowane na komputerach dedykowanych stanowiących bramę (ang. *gateway*) do chronionej sieci, np. SEAL (DEC), Interlock (ANS), Gauntlet (TIS) czy Firewall-1 (Checkpoint Technology);
- sprzęt–mosty dzięki możliwości „uczenia się" topologii adresów, a przez to filtrujące ruch w sieci oraz routery, które z założenia mogą filtrować i rejestrować adresy źródeł i przeznaczenia przesłań.

W sieci Internet jest dostępny modularny zestaw narzędzi do tworzenia zindywidualizowanych „kurtyn ogniowych" – *Firewall Toolkit* firmy *Trusted Information Systems Inc.*

Inną metodą kontroli dostępu (identyfikacji) jest „oddzwanianie" (ang. *call-back*), polegające na tym, że system, do którego zgłasza się użytkownik podając konto i hasło, inicjuje właściwą transmisję, zwracając się pod właściwy dla tego użytkownika adres (numer) zapamiętany w zweryfikowanym przez administratora zbiorze.

Przechowywanie danych

W sieciach LAN stosowanym rozwiązaniem sprzętowym są bezpieczne rozgałęziacze LAN (ang. *secure hub*) szyfrujące ramki przesłania przekazywane do użytkowników nie będących adresatami sieci lub inteligentne – przełączające (*ng. intelligent/switching hub*), kierujące do portu użytkownika tylko ramki zawierające jego adres.

Dość powszechną metodą unikania „koni trojańskich" – ukrytych, doklejonych procedur do programów systemowych służących np. do łamania zabezpieczeń przez przechwytywanie nazw kont i haseł (ang. *sniffing*) – jest opatrywanie ich sumami kontrolnymi, generowanymi za pomocą złożonych algorytmów, np. MD5.

Innym, zyskującym uznanie rozwiązaniem problemu przechwytywania jest stosowanie haseł jednokrotnych – kroczących (ang. *one-time password*).

Bezpieczeństwo w sieci Internet

Internet, który do niedawna był dość powszechnie uznawany za niewłaściwy dla przesyłania danych, nawet tych o niskim stopniu poufności, może okazać się w niedalekiej przyszłości – po upowszechnieniu się odpowiednich narzędzi zabezpieczających – właściwym medium do realizacji tego rodzaju przesłań. Ostatnio wprowadzonymi narzędziami podnoszącymi poziom zaufania do Internetu jest produkt firmy *Mosaic Communication Co. – Netscape*, wyposażony we własne funkcje szyfrujące i identyfikacji serwerów, oraz *Netsite* – bezpieczny serwer internetowy. Produkty te współpracując umożliwiają realizację bezpiecznych transakcji przez Internet.

Standaryzacja objęła także obszary bezpieczeństwa Internetu – trwają prace nad standardową bezpieczną postacią oprogramowania Mosaic, tzw. Secure HTTP (*Hypertex Transfer Protocol*).

Normy

POSIX 1003.6 – podstawowe reguły bezpieczeństwa dla systemu operacyjnego;
ISO 7498-2 OSI (*Security Architecture*) – określa podstawowe zasady bezpieczeństwa w systemach realizowanych zgodnie z modelem OSI. Architektura ta jest opisywana następującymi standardami:

- TLSP (*Transport Layer Security Protocol*) – ISO DIS 10736 wykorzystujący standardowy ISO 8073 i 8602;
- SILS (Secure Interoperable LAN Standard) – IEEE 802.10;
- PLE (Physical Layer Encryption – ISO 9160;
- NLSP (Network Layer Security Protocol) – ECMA oraz w warstwach wyższych: ASE, STS (ISO); ECMA APAS czy X.509.
- ISO 8731/2 – wysoko wydajny algorytm (MAA – *Message Authentication Algorithm*) tworzenia 32-bitowego kodu potwierdzenia komunikatu (MAC – *Message Authentication Code*);
- X9.9 i ISO 8730 – MAC;
- X9.17 – zarządzanie kluczami;
- X9.31 – podpis cyfrowy;
- ISO 8731/1 oraz 8372 – DEA (*Data Encryption Algorithm*) algorytm symetrycznego szyfrowania zgody z DES (*Data Encryption Standard*); DES przyjęty przez ANSI jako X3.106 i X3.93 używa 56-bitowych kluczy do szyfrowania–deszyfrowania 64-bitowych ciągów danych;
- X.509 – *Directory Authentication* – mechanizm zabezpieczeń dla systemów wykorzystujących normę X.500;
- X.400 MHS *Security* – zabezpieczenia dla systemu poczty elektronicznej OSI.

W dziedzinie stwierdzania tożsamości (ang. *authentification*) użytkowników wyraźną przewagę zyskują rozwiązania stosujące inteligentne (zawierające mikroprocesor) karty identyfikacyjne (ang. *smart card*). Norma obowiązująca w odniesieniu do nich została opracowana przez ISO i ma numer 7816 (poziom 1, 2 i 3). Dokumenty normalizujące poziomy wyższe m.in. API, znajdują się obecnie w opracowaniu.

XI KONFERENCJA

XI Konferencja

Informatyka w szkole

Przewodnim tematem Konferencji, która odbędzie się w dniach 13–16 **września 1995 r. w Kielcach, na Politechnice Świętokrzyskiej** jest hasło:

KOMPUTER JAKO ŚRODEK POROZUMIEWANIA SIĘ

Organizatorami Konferencji są Instytut Informatyki Uniwersytetu Wrocławskiego, Politechnika Świętokrzyska w Kielcach i Ministerstwo Edukacji Narodowej.

W programie Konferencji są przewidziane: wykłady plenarne zaproszonych gości (m.in. na temat sieci komputerowych w nauczaniu), obrady w sesjach tematycznych (nt. nauczania przedmiotu *elementy informatyki*, miejsca komputerów w pedagogice i w szkolnictwie specjalnym, stosowania komputerów w nauczaniu matematyki, fizyki, przedmiotów przyrodniczych i przedmiotów zawodowych oraz wykorzystania sieci komputerowych w szkole i w nauczaniu) oraz prezentacje plakatów, sprzętu komputerowego i oprogramowania.

Większość uczestników tego cyklu konferencji stanowią nauczyciele ze szkół średnich i wyższych oraz przedstawiciele instytucji związanych z edukacją.

Do udziału w Konferencji Organizatorzy zapraszają również firmy i instytucje zaopatrujące szkoły i oferujące wydawnictwa szkolne, sprzęt komputerowy oraz oprogramowanie narzędziowe i edukacyjne. Konferencja jest bowiem okazją do zaprezentowania oferty i poglądów firm na edukację informatyczną przedstawicielom szkół i uczelni z całego kraju.

Dokładniejsze informacje dotyczące warunków uczestnictwa oraz form udziału firm w Konferencji można uzyskać w **Instytucie Informatyki Uniwersytetu Wrocławskiego, ul. Przesmyckiego 20, 51-151 Wrocław; tel.: 25-12-71, 247-382; fax: 25-12-71;**
e-mail: syslo@ii. uni. wroc. pl.

Koncepcja realizacji poczty elektronicznej X.400 w TP S.A.

Sławomir Michalski
Marian Suskiewicz
Telekomunikacja Polska S.A.
Warszawa

Poczta elektroniczna (ang. *e-mail*) jest popularną nazwą usług zaliczanych do usług dodanych. Usługa ta oferuje użytkownikom szybką wymianę informacji zwanych wiadomościami z wykorzystaniem komputerów i mediów teletransmisyjnych.

Poczta elektroniczna oferuje dużo większe możliwości niż tradycyjne formy międzyludzkiej komunikacji, gdyż jest usługą:

- asynchroniczną, tzn. nie wymaga się, aby odbiorca wiadomości był aktywny (*on-line*) wtedy, gdy wiadomość przychodzi,
- wieloadresową, tzn. pozwala zaadresować wiadomość do wielu odbiorców i przekazać tę wiadomość jednocześnie do wskazanych adresatów,
- otwartą, tzn. pozwala na wymianę informacji z innymi systemami przesyłania, np. teleksem, telefaksem itp.

Telekomunikacja Polska S.A. – największy publiczny operator telekomunikacyjny w Polsce – postanowiła rozszerzyć swoje usługi właśnie o elektroniczną wymianę informacji opartą na standardzie X.400. Po przeprowadzeniu badań marketingowych stwierdzono coraz większe zainteresowanie taką usługą w Polsce i postanowiono zakupić odpowiedni system komputerowy realizujący tę usługę.

Publiczny System Wymiany Wiadomości MHS (*Message Handling System*) otrzymał nazwę POLKOM 400, co historycznie nawiązuje do eksploatowanego wcześniej w telekomunikacji Systemu Retransmisji Faksów, Teleksów i Telegramów – POLKOM. W stosunku do swego poprzednika, obecny system ma całkowicie nową jakość realizacji usług publicznych i poza nazwą niewiele wspólnego ma z dawnym POLKOM-em. W wyniku przeprowadzonego przetargu na Publiczny System Wymiany Wiadomości MHS, oparty na standardzie X.400, TP S.A. wybrała jako integratora i dostawcę, francuską firmę SYSECA. Zaproponowany przez tę firmę system POLKOM 400 opiera się na produktach znanego na świecie dostawcy systemów wymiany informacji – firmy ISOCOR. System ten stanowi kompletne rozwiązanie, zarówno dla operatora publicznego, jak i dla użytkownika końcowego.

System POLKOM 400

System POLKOM 400 oparto generalnie na standardzie X.400 (84/88/92), który definiuje Publiczny System Wymiany Wiadomości MHS i następujące protokoły wymiany przesyłek:

- P1 między węzłami pocztowymi MTA (*Message Transfer Agent*),
- P2 między modułami obsługi użytkowników UA (*User Agent*),
- P3 między użytkownikami a węzłami pocztowymi MTA,
- P7 między użytkownikami a pamięcią wiadomości MS (*Message Store*), w której są przechowywane skierowane do nich przesyłki.

System określa także sposób dostępu najbardziej rozpowszechnionej usługi realizowanej w sieciach komputerowych – poczty elektronicznej – do innych systemów przesyłania wiadomości. Ponadto opisuje elementy koperty elektronicznej, na której umieszczony jest znormalizowany adres nadawcy i odbiorcy oraz takie cechy, jak np. pilność, stopień poufności, termin ważności itp.

W kolejnej wersji standard X.400 został wzbogacony o elementy bezpieczeństwa zapewniające m.in. uwiarygodnienie nadawcy i odbiorcy oraz bezbłędne przesyłanie. Ponadto zdefiniowano w nim sposób dołączenia do systemu X.400 takich usług, jak usługa teleksowa, faksowa czy fizyczne doręczenie, polegające na wydrukowaniu i dostarczeniu przesyłki adresatowi, do którego dotarcie inną drogą nie jest możliwe.

Architektura systemu

System POLKOM 400 zostanie dostarczony w przedstawionej na rys. 1 następującej konfiguracji sprzętowej:

- serwer główny:
  - Stratus R5 Risc Fault Tolerant Computer – z dwoma procesorami,
  - 2 × 64 MB RAM,
  - 4 × 1,4 GB HDD (*disk duplexing*),
  - 2 Gb DAT (*backup cartridge*),
  - 4 × K118-D12 (64 Kb/s),
  - 2 × K124 (2 Mb/s),
  - 32 porty asynchroniczne (19.2 Kb/s),
- serwer komunikacyjny do innych systemów wymiany informacji (PC UNIX/SCO),
- stanowisko zarządzania systemem (PC/Windows),
- podsystemy współpracy z abonentami sieci teleksowej i faksowej (DISTEL),
- moduły obsługi użytkowników (RUA/P7),
- interfejsy dostępowe (X.25, ASYNC, PAD, ISDN).

Podstawowe moduły systemu

Oparty na oprogramowaniu firmy ISOCOR system POLKOM 400 ma budowę modularną. W jego skład

wchodzą następujące moduły podstawowe:

- MTA ISOPLEX ADMD,
- MS ISOPLEX MS,
- X.500 ISOPLEX DS,
- ISOGATE (cc: Mail, Ms: Mail, Novell-MHS, Lotus Notes, SMTP),
- ISOTRADE (moduł EDI – *Electronic Data Interchange*),
- ISOMAN (moduł administracji i zarządzania),
- AU (ISOTELEX, ISOFAX, ISOROUTE),
- UA (LUA, RUA, Sec RUA),
- API (MAPI, SSAPI, XOPEN, XDS, FPI),
- ACCOUNTING, BILLING, STATISTICS, ALARMS.

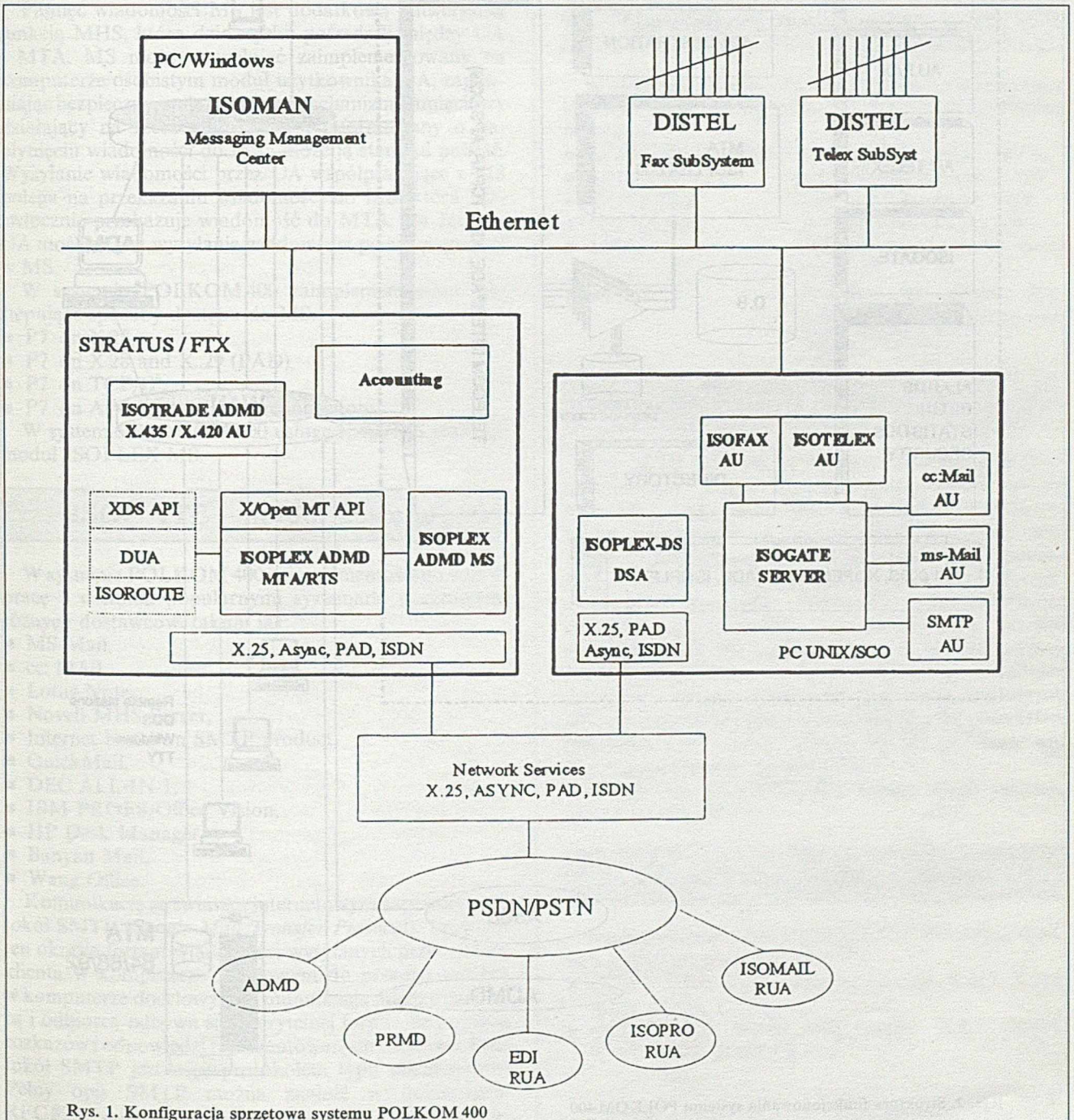
Struktura funkcjonalna systemu POLKOM 400 została przedstawiona na rys. 2.

Moduł MTA Isoplex 800

Moduł przekazywania wiadomości MTA odpowiada za transport komunikatów między węzłami systemu X.400. Jest on odpowiednikiem urzędu pocztowego sortującego korespondencję. Korespondencja wychodząca jest umieszczana w odpowiedniej skrytce pocztowej, jeśli odbiorca jest obsługiwany przez dany moduł, w przeciwnym wypadku, jeżeli adresat nie jest lokalny, wiadomość jest transportowana do innych MTA. Głównym środkiem transportu jest sieć transportowa, a punktem docelowym – właściwy dla adresata zdalny MTA.

W systemie POLKOM 400 wiadomości mogą być przesyłane po sieci za pomocą następujących protokołów komunikacyjnych:

- RFC 1006 on TCP/IP
- ISO CLNS on 802.3,
- ISO CONS on X.25,



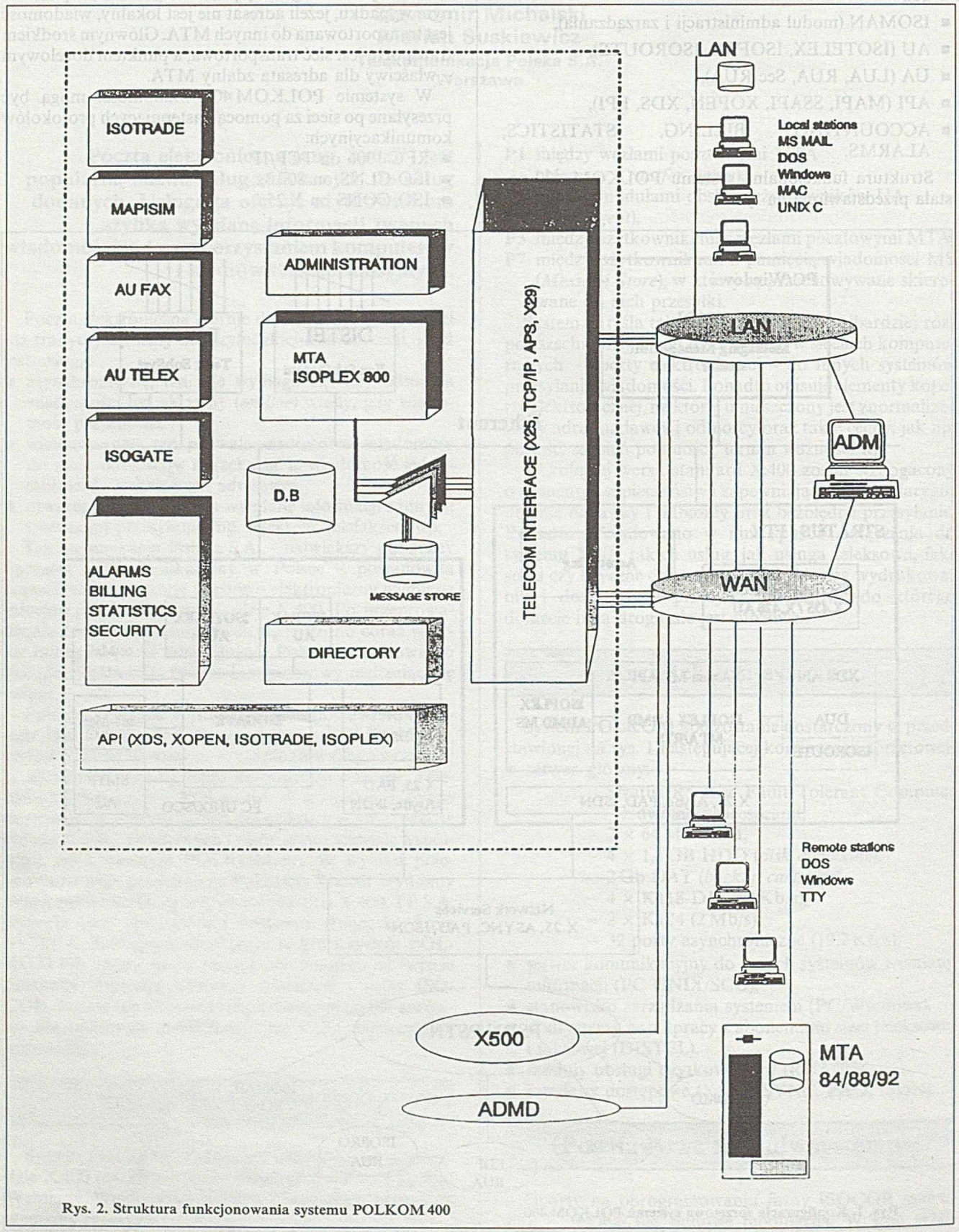
Rys. 1. Konfiguracja sprzętowa systemu POLKOM 400

- Asynchronous with calling mode on PAD X.3/X.28/X.29,
- APS on asynchrone connections,
- Frame relay.

Moduł MTA Isoplex 800 jest całkowicie obsługiwany przez administratora systemu.

UA – moduł obsługi użytkownika

Moduł obsługi użytkownika działa jak skrzynka pocztowa rozumiana wg zasad amerykańskich, tzn. podobnie jak w Europie poczta przychodząca jest przechowywana do momentu jej odebrania przez adresata i odmien-



Rys. 2. Struktura funkcjonowania systemu POLKOM 400

nie jak w Europie, w tej samej skrzynce można umieszczać korespondencję do wysłania.

Użytkownik systemu POLKOM 400 postrzega moduł UA przez jego oprogramowanie obsługujące dialog. Moduł użytkownika UA wykonuje wszystkie funkcje związane z przygotowaniem, wysłaniem i odbiorem wiadomości. Obejmuje to takie funkcje, jak przypomnienie wypełnienia pól adresu, tematu i treści wiadomości oraz np. funkcje redakcji tekstu. Do zadań UA należy również ułatwienie użytkownikowi manipulacji wiadomościami odebranymi z MTA.

W systemie POLKOM 400, poza dowolnymi UA komunikującymi się za pomocą protokołu P7, występują dwa dodatkowe UA firmy ISOCOR:
- graficzny ISOPRO (GUI for Windows 3.1 and NT),
- znakowy ISOMAIL 800 (for DOS).

MS – moduł pamięci wiadomości

Pamięć wiadomości MS jest dodatkową uniwersalną funkcją MHS, która działa jako pośrednik między UA i MTA. MS może uzupełniać zaimplementowany na komputerze osobistym moduł użytkownika UA, zapewniając bezpieczny, stale dostępny mechanizm pamięciowy działający na rzecz UA. UA jest informowany o napłynięciu wiadomości do MS i może ją stamtąd pobrać. Wysyłanie wiadomości przez UA współpracujące z MS polega na przekazaniu wiadomości do MS, która bezzwłocznie przekazuje wiadomość do MTA. Na żądanie UA możliwe jest wysyłanie wiadomości przechowywanej w MS.

W systemie POLKOM 400 zaimplementowano następujące sposoby dostępu do MS:
- P7 on X.25,
- P7 on X.28 and X..29 (PAD),
- P7 on TCP/IP,
- P7 on APS asynchronous connections.

W systemie POLKOM 400 usługę X.400 MS realizuje moduł ISOPLEX MS.

ISOGATE – moduł dostępu

W systemie POLKOM 400 zaimplementowano współpracę z wieloma popularnymi systemami pocztowymi różnych dostawców, takimi jak:
- MS-Mail,
- cc: MAil,
- Lotus Notes,
- Novell MHS Server,
- Internet based on SMTP product,
- QuickMail,
- DEC ALL-IN-1,
- IBM PROFS/Office Vision,
- HP Desk Manager,
- Banyan Mail,
- Wang Office.

Komunikację ze światem internetowym zapewnia protokół SMTP (*Simple Mail Transfer Protocol*). Protokół ten określa format wiadomości wysyłanych przez proces klienta w komputerze źródłowym do procesu serwera w komputerze docelowym. Komunikacja między nadawcą i odbiorcą odbywa się w czytelnej formie, za pomocą rozkazów i odpowiedzi reprezentowanych tekstowo. Protokół SMTP jest więc protokołem typu klient-serwer. Pełny opis SMTP można znaleźć w dokumencie RFC 822. Natomiast w dokumencie RFC 1090 jest opisany standard stosowania protokołu SMTP w sieciach X.25, a w dokumencie RFC 1006 – w sieciach TCP/IP. Wszystkie te dokumenty zostały zaimplementowane m.in. w module ISOGATE systemu POLKOM 400.

Moduły ISOTELEX i ISOFAX

Od wielu lat używane są dwa tradycyjne systemy elektronicznego przesyłania informacji: teleks i faks. Teleks działa jako autonomiczna sieć z własnymi centralami, umożliwiająca przekazywanie informacji reprezentowanej w bardzo ograniczonym zbiorze znaków i z małą szybkością (standardowo 50 bodów). Faks natomiast wykorzystuje do przesyłania dokumentów normalną publiczną komutowaną sieć telefoniczną. Usługa ta ma także bardzo istotne ograniczenia. W systemie POLKOM 400 zaimplementowano dostęp zarówno do sieci teleksowej, jak i faksowej.

Interfejsy programowe – APIs

W systemie POLKOM 400 dostępne są następujące interfejsy programowe APIs (*Application Programming Interface*):
- API ISOPLEX 800 – interfejs programowy MTA,
- API XDS++ – interfejs programowy X.500,
- ISOTRADE – interfejs programowy EDI,
- API X/Open – interfejs programowy UA,
- MAPI – interfejs programowy firmy Microsoft,
- SSAPI – Security profile provider, Key store provider, Algorithm provider.

Elektroniczny spis abonentów – X.500

Aby MHS X.400 mógł się stać systemem o zasięgu globalnym, konieczne było rozwiązanie problemu implementacji i utrzymania elektronicznego spisu użytkowników. Zagadnienie to jest przedmiotem zaleceń serii X.500, definiujących model funkcjonalny spisu abonentów. Spis jest zbiorem otwartych systemów współpracujących przy utrzymywaniu logicznej bazy danych o zbiorze obiektów realnego świata. Użytkownicy spisu, którymi mogą być osoby lub programy, mają możliwość odczytu i modyfikacji informacji pod warunkiem posiadania uprawnień. Podczas dostępu do spisu każdy użytkownik jest reprezentowany przez moduł dostępu do spisu DUA (*Directory User Agent*). Moduł ten jest procesem aplikacyjnym w sensie modelu OSI.

W systemie POLKOM 400 usługę X.500 realizuje moduł ISOPLEX DS.

Standardy i profile systemu

Funkcjonowanie systemu POLKOM 400 będzie zgodne z następującymi zaleceniami:
- CCITT X.200 Model odniesienia OSI, X.213, X.214, X.215, X.224, X.225,
- CCITT X.400 Model funkcjonalny X.400, X.401, X.409, X.410, X.411 i X.420,

dokończenie na s. 31

Systemy logistyczne wyzwaniem dla informatyków

Stefan Abt
Akademia Ekonomiczna
Poznań

Przystępując do intensyfikacji rozbudowy sieci komputerowych w Polsce oraz do rozwoju telekomunikacji warto zwrócić uwagę na logistykę, która może się stać nadrzędnym kryterium oceny przydatności i efektywności określonego typu konfiguracji sprzętowych, a także może służyć wytyczeniu kierunków przyszłościowego rozwoju informatyki.

Wobec coraz bardziej masowej produkcji, a także stopniowo rozwijanej skali dystrybucji towarów, pojawiła się potrzeba wyodrębnienia logistyki, jako procesu zarządzania całymi łańcuchami dostaw. To dość ogólne określenie w zakresie teorii oraz wdrożeń praktycznych nabiera różnych wymiarów w zależności od sytuacji gospodarowania dobrami.

Logistyka staje się obecnie tą dziedziną wiedzy, która opierając się na bazie systemów informatycznych zmierza ponad podziałami organizacyjnymi przedsiębiorstw ku ich integracji, by zapewnić optymalne kształtowanie łańcuchów zaopatrzeniowych od momentu pozyskania surowców, przez ich przetworzenie, dystrybucję w różnych ogniwach handlu, aż do dostarczenia ostatecznemu nabywcy [3]. Tak rozumiane docelowe łańcuchy logistyczne wymagają czasu na ich przygotowanie i zbudowanie. Obecnie w Polsce znajdujemy się na etapie szczególnego zainteresowania logistyką ze strony przedsiębiorstw, które w warunkach gospodarki rynkowej zostały zmuszone do bardziej rentownej działalności. Logistyka staje się więc okazją do zmodernizowania zarządzania, podkreślając przede wszystkim potrzebę uwzględniania strategii rozwoju logistycznego, w którym z równą troską, jak o przepływ towarów, dba się o właściwy przepływ informacji i ich należyte wykorzystanie dla kompleksowej optymalizacji. Należy dodać, że koncepcje logistyczne są nie tylko szansą, ale wręcz wymogiem czasów, gdy procesy związane z wymianą towarową stają się coraz bardziej złożone, zwiększa się ich skala, a konieczność dostosowania się do potrzeb i wymagań nabywców idzie w parze z przymusem obniżki kosztów.

Systemy logistyczne wyzwaniem dla gospodarki

Dla praktyki gospodarczej niezbędne jest wyjście naprzeciw wielu zespołom kierowniczym w przedsiębiorstwach przemysłowych, transportowych, handlowych i innych, aby przekonały się one o celowości wdrażania koncepcji logistycznych i o tym, że istnieje wiele gotowych rozwiązań, na poziomie przyjaznego dla użytkowników oprogramowania komputerów. Wystarczy tylko przygotować się do wdrożeń i przyjąć strategię nowoczesnego zarządzania. Rodzi się też teoria logistyki, mająca swe źródła w nowoczesnych metodach organizacji i zarządzania. Sięga ona do kompleksowego rachunku kosztów, a przede wszystkim do informatyki gospodarczej wraz z jej nieustannie doskonalonymi możliwościami automatycznej identyfikacji oraz symulacji komputerowej. Logistyka stanowi jednak już samodzielną dziedzinę badawczą, której przedmiotem stały się systemy logistyczne. Systemy te należy rozpatrywać w ujęciu kompleksowym, począwszy od wyników badań marketingowych, określających zapotrzebowanie na produkty określonej jakości, następnie przez wszystkie ogniwa tworzące łańcuch logistyczny, tj. produkcję, magazynowanie, przetwórstwo, transport i zbyt realizowany różnymi kanałami dystrybucji, a kończąc na konsumencie.

Budowa systemów logistycznych wymaga zespolonej pracy wielu uczestników gospodarowaia, m.in. banków, które docelowo zostaną również dołączone do sieci komputerowych tych systemów. Wobec znacznie rozbudowanego zakresu systemów logistycznych jest konieczne wyodrębnienie podsystemów, dających pogląd na etapowość dokonywania wdrożeń. Zintegrowanie takich podsystemów zmierza do stworzenia w ramach łańcuchów zaopatrzenia zintegrowanych systemów informatycznych, umożliwiających optymalizację dostaw (m.in. przez symulację komputerową, automatyczną identyfikację towarów oraz kompleksowy rachunek ekonomiczny). Dotyczy to problemów zaopatrzeniowych wielkiej skali i pozwala na stosowanie najnowszych metod zaopatrzenia materiałowego zgodnie z zasadą *Just-in-Time*, tj. dokładnie na czas. Umożliwia to zmniejszanie zapasów do minimum i dzięki temu osiąganie znacznych oszczędności. Różnorodność systemów logistycznych uzmysławia ich umiejscowienie w łańcuchach magazynowo-transportowych (rys. 1), we wszystkich można jednak wyróżnić istotne elementy składowe, tj. węzły i ścieżki sieci zaopatrzeniowej, rozpatrywanej w dwu warstwach: fizycznej (ludzi i zasobów) oraz informacyjnej (ilościowego i wartościowego ujęcia procesów gospodarczych).

W ujęciu bardziej praktycznego języka, elementami systemu logistycznego są:

- zintegrowane sieci komputerowe, umożliwiające zdążanie do automatycznego wspomagania zarządzania, gdzie informatyka stanowi istotne narzędzie realizacji celu, jakim jest systemowe rozwiązanie sterowania obiegiem materiałowo-finansowym;
- środki techniczne, umożliwiające przemieszczanie, przeładunek i magazynowanie towarów w cyklach zaopatrzeniowych, od powstania produktu do jego odbioru przez konsumenta (rys. 2);
- służby decyzyjne, zarządzające fizycznym przemieszczaniem towarów, z zastosowaniem nowoczesnych narzędzi (optymalizacji wielokryterialnej i symulacji), zorganizowane w odpowiednich komórkach.

Komputeryzację wspomagającą zarządzanie przedsiębiorstwami oraz wprowadzanie kodów kreskowych można uznać za wielkie przedpole logistyki, choć wdrożenia te nie za-

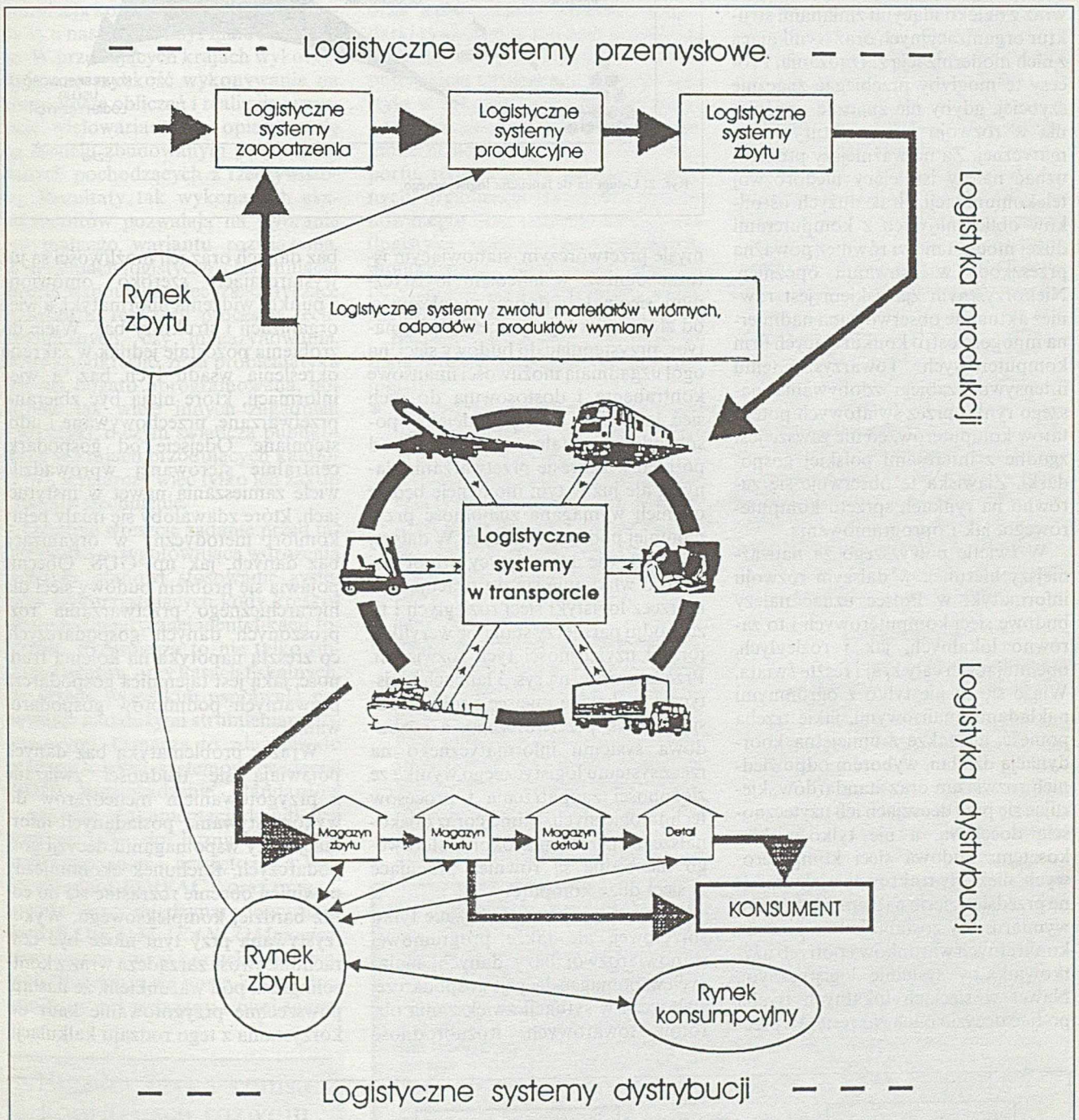
wsze mają w swej strategii w Polsce założenia i wymogi systemów logistycznych, z pełnym wykorzystaniem ich możliwości [1]. Z punktu widzenia logistyki należy wyraźnie rozgraniczyć dwie warstwy analityczne, tj. przepływ towarów i przepływ informacji, z odpowiednio nowoczesną nadbudową. Jako filary przyszłych systemów logistycznych, wymienić można **w zmodernizowanym logistycznie przepływie towarów:**

- nowoczesną gospodarkę magazynową,
- unowocześniony transport,
- stosowanie automatycznej identyfikacji,
- zmodernizowaną gospodarkę zapasami,
- optymalizację kosztów,

natomiast **w zmodernizowanym przepływie informacji:**

- stosowanie modeli decyzyjnych,
- odpowiednią infrastrukturę informatyczną,
- używanie metod kontrolingu,
- wykorzystanie metod symulacji komputerowej,
- przechodzenie na elektroniczną wymianę danych (EDI).

Tak pojmowane systemy logistyczne można budować w skali mikro, a więc dla różnego typu przedsiębiorstw, a także w skali makro. Zintegrowana całość będzie stanowić przyszłościowe nowoczesne systemy zarządzania. Stopień rozbudowy poszczególnych elementów systemów logistycznych wpływa na daleko idącą różnorodność rozwiązań logistycznych, w tym także samych systemów. Docelowo systemy logistyczne obe-



Rys. 1. Systemy logistyczne i ich struktura

jmą zarówno procesy produkcji, jak i dystrybucję, choć aktualnie celowe wydaje się rozróżnianie logistyki produkcji i logistyki dystrybucji, co wynika z odmienności specyfiki stosowanych metod.

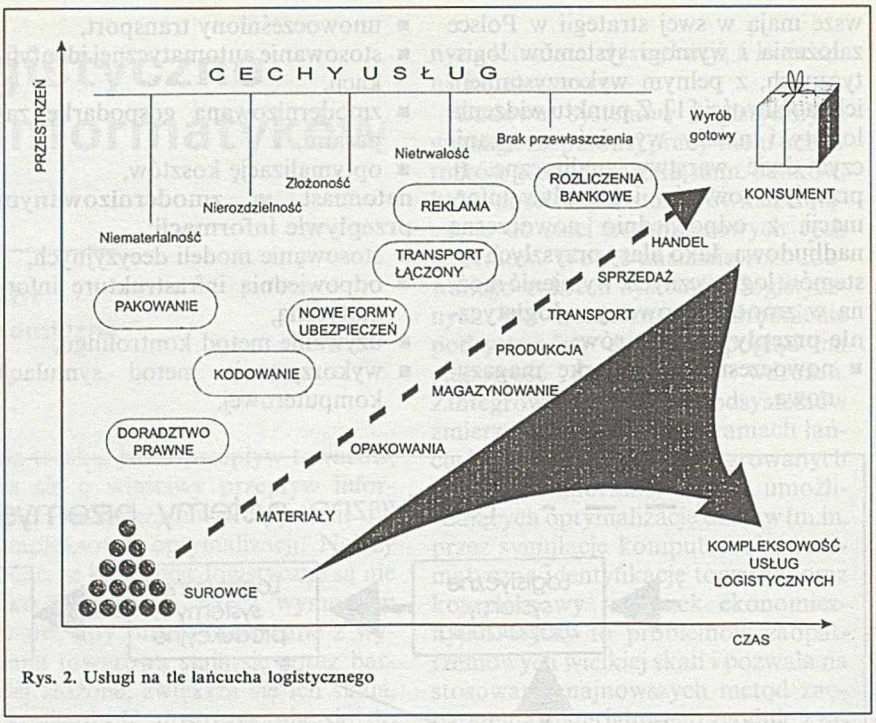
Aktualne kierunki komputeryzacji

Przechodzenie w Polsce na gospodarkę rynkową wymusiło dokonywanie przekształceń własnościowych, wraz z daleko idącymi zmianami struktur organizacyjnych oraz wynikającą z nich modernizacją zarządzania. Procesy te mogłyby przebiegać znacznie szybciej, gdyby nie znaczne opóźnienia w rozwoju infrastruktury informatycznej. Za najważniejszy problem uznać należy istniejący niedorozwój telekomunikacji. Brak dużych ośrodków obliczeniowych z komputerami dużej mocy stanowi również poważną przeszkodę w usuwaniu opóźnień. Niekorzystnym zjawiskiem jest również aktualnie obserwowana nadmierna mnogość ostro konkurujących firm komputerowych. Towarzyszą temu intensywne zabiegi zdobywania naszego rynku przez światowych potentatów komputerów, co nie zawsze jest zgodne z interesami polskiej gospodarki. Zjawiska te obserwuje się zarówno na rynkach sprzętu komputerowego, jak i oprogramowania.

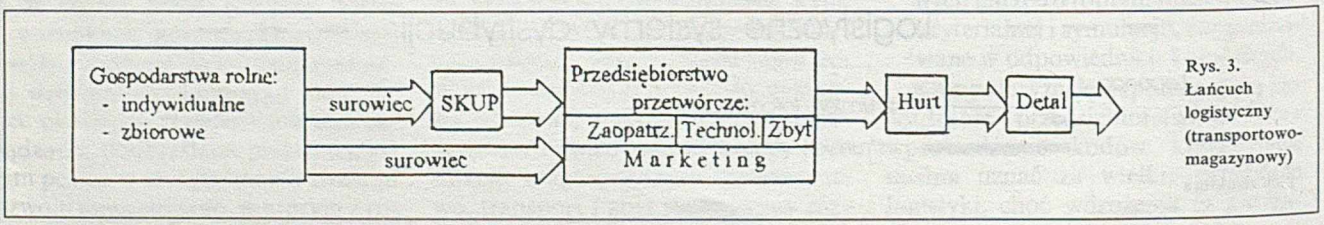
W świetle powyższego za najważniejszy kierunek w dalszym rozwoju informatyki w Polsce uznać należy budowę sieci komputerowych i to zarówno lokalnych, jak i rozległych, obejmujących cały kraj i resztę świata. Wiąże się to nie tylko z ogromnymi nakładami finansowymi, jakie trzeba ponieść, ale także z umiejętną koordynacją działań, wyborem odpowiednich rozwiązań oraz standardów, kierując się przy decyzjach ich użytecznością docelową, a nie tylko niskim kosztem. Budowa sieci komputerowych, niekiedy traktowana jako modne przedsięwzięcie nabiera właściwego wymiaru, gdy zostanie odniesiona do konkretnych warunków i potrzeb użytkownika w systemie logistycznym. Nawet w sieciach lokalnych trzeba podjąć decyzje o ich zakresie. W przemyśle przetwórczym, stanowiącym istotne ogniwo w łańcuchu logistycznym, sieć należy dobrać w zależności od złożoności tego procesu. Informatycy, przystępując do budowy sieci, na ogół uzgadniają możliwości finansowe kontrahenta i dostosowują do nich sieć. Jeżeli chcą do tego podejść w sposób odpowiedzialny, winni wyjść od potrzeb w zakresie przetwarzania danych, ale już w tym momencie będzie od nich wymagana znajomość przynajmniej podstaw logistyki. W dalszej perspektywie informatycy winni zadbać o włączanie się do pracujących na rzecz logistyki sieci rozległych i tu zachodni partnerzy staną się weryfikatorami użyteczności tych rozwiązań. Przedstawiony na rys. 3 łańcuch logistyczny pokazuje miejsce i rolę przedsiębiorstwa przetwórczego, a rozbudowa systemu informatycznego na rzecz systemu logistycznego wynika ze złożoności zaopatrzenia i procesów technologicznych. Mimo coraz doskonalszego sprzętu mikrokomputerowego niezbędne są również pracujące w sieci duże komputery.

Odrębny problem natury nie tylko sprzętowej, ale także programowej stanowi rozwój bazy danych, mających wspomagać decyzje gospodarcze, zwłaszcza w sytuacji zwiększania obrotów towarowych. Różnorodność baz danych oraz ich możliwości są już wystarczająco szeroko omówione z punktu widzenia informatyki, a więc organizacji i struktury baz. Wiele do zrobienia pozostaje jednak w zakresie określenia wsadu tych baz, a więc informacji, które mają być zbierane, przetwarzane, przechowywane i udostępniane. Odejście od gospodarki centralnie sterowanej wprowadziło wiele zamieszania nawet w instytucjach, które zdawałoby się miały pełny komfort metodyczny w organizacji baz danych, jak np. GUS. Obecnie pojawia się problem budowy sieci dla hierarchicznego przetwarzania rozproszonych danych gospodarczych, co zresztą napotyka na kolejną trudność, jaką jest tajemnica gospodarcza prywatnych podmiotów gospodarowania.

Wraz z problematyką baz danych pojawiają się trudności związane z przygotowaniem menedżerów do wykorzystywania posiadanych informacji przy wspomaganiu decyzji gospodarczych. Rachunek ekonomiczny powinien obecnie rozrastać się do coraz bardziej kompleksowego. Wykorzystywana przy tym może być tzw. rachunkowość zarządcza wraz z kontrolingiem, pod warunkiem, że nastąpi powszechne przygotowanie kadr do korzystania z tego rodzaju kalkulacji.



Rys. 2. Usługi na tle łańcucha logistycznego



Rys. 3. Łańcuch logistyczny (transportowo-magazynowy)

Ta problematyka również należy do informatyki, gdyż w praktyce zdecydowanie za mało wykorzystywane są takie narzędzia, jak np. arkusze kalkulacyjne, a przecież obecnie dysponuje się pakietami programowymi zapewniającymi korzystanie z baz danych, edytorów i grafiki (np. MS WORKS). Ich powszechne stosowanie na sprzęcie mikrokomputerowym będzie ogromnym sukcesem, ale pozostanie jeszcze do zrealizowania trudny problem zdalnej współpracy z bazami.

Specyficzny, bardzo przydatny logistyce kierunek rozwojowy, stanowi symulacja komputerowa, której metody są u nas jeszcze zbyt mało stosowane. W przodujących krajach wykorzystują one szybkość wykonywania na komputerze obliczeń i realizują symulację wielowariantowo, opierając się na modelu zbudowanym przy użyciu danych pochodzących z rzeczywistości. Rezultaty tak wykonanych eksperymentów pozwalają na wybranie optymalnego wariantu rozwiązania. W systemach logistycznych symulacją można wspomagać decyzje dotyczące transportu, realizacji procesów technologicznych, czy magazynowania. Warto podkreślić, że ta problematyka jest już bogato oprogramowana, podobnie jak wiele innych zagadnień z logistyki, o czym świadczą publikowane w krajach przodujących katalogi [4], wystarczy więc tylko ich zakup i rozpowszechnienie.

Ostatnie wreszcie zadanie przed informatyką przygotowującą wdrożenia logistyki, stanowi stosowanie systemów wykorzystujących kody kreskowe do automatycznej identyfikacji towarów. Przyspiesza to nie tylko obsługę klientów przy kasach fiskalnych, ale przede wszystkim usprawnia panowanie nad dużymi strumieniami towarowymi. Oznacza to zdążanie do bezpapierowych systemów ewidencji (EDI). Wprowadzenie standardów w zakresie dokumentacji handlowej doprowadziło do licznych porozumień i uzgodnień – przyjęto już w Polsce standard EDIFACT oraz przygotowano nowy międzynarodowy standard EANCOM (*EANCOMmunication*), stosowany w krajach przodujących. Pojawiają się nowe kody i doskonalony jest związany z nimi sprzęt.

Eurologistyka szansą koordynacji rozwoju

Niezależnie od różnych kierunków rozwoju logistyki światowej, zdążanie Polski do Unii Europejskiej wymaga szybkiego przystosowania się przynajmniej do wymogów dyktowanych przez kraje europejskie. Partnerstwo z gospodarką europejską wymaga nie tylko zbudowania odpowiedniej infrastruktury informatycznej, ale także pilnego przygotowania przedpola logistycznego, zgodnie z wymogami eurologistyki ingerującymi w wiele dziedzin zarządzania. Eurologistyka zajmuje się bowiem przemianami związanymi z utworzeniem Wspólnego Rynku EWG. Przemianami tymi są nowe warunki współdziałania w podziale pracy w sferze międzypaństwowej oraz wprowadzenie struktur gospodarki rynkowej w Europie Środkowej i Wschodniej [2]. Pośrednio z komputeryzacją związane są wymogi logistyki w zakresie infrastruktury transportu (przekształcenia własnościowe, modernizacja dróg i środków transportu, reorganizacja przejść granicznych, organizacja transportu kombinowanego) oraz ochrony środowiska (logistyka miejska, agro-ekosystem, modernizacja opakowań, budowa oczyszczalni ścieków, ekologia lokalizacji obiektów).

Bezpośredni związek z informatyką mają również pozostałe wymogi eurologistyki:

- budowa otwartych sprzętowo sieci informatycznych w środowisku Windows, organizacja centrów informacji rynkowej, a w dalszej perspektywie nowoczesnych baz danych gospodarczych, popularyzacja ujednoliconego oprogramowania użytkowego (np. dla systemów sklepowych), modelowanie gospodarki rynkowej;
- budowa centrów dystrybucji, stanowiących istotne ogniwo łańcuchów logistycznych z nowoczesnym wyposażeniem informatycznym oraz zastosowaniem automatycznej identyfikacji towarów, rozwój systemów eksperckich niezbędnych przy procesach decyzyjnych w ww. centrach, optymilizacja lokalizacji centrów dystrybucji;
- przygotowanie standardów norm w zakresie: technologii przetwarzania danych i łącz komputerowych, norm ISO-9000, terminologii logistycznej, systemów bezpapierowej dokumentacji (EDI-EANCOM);
- logistyki w produkcji, zmierzającej do modernizacji technologii, wprowadzania automatyzacji, podwyższenia jakości wyrobów, rozwoju partnerskiej kooperacji, gwarantującej krajowi politykę proeksportową.

Powyższe wymogi warunkujące wejście do Wspólnoty Europejskiej przez systemy logistyczne wymagają ukierunkowania prac informatycznych głównie na te problemy. Podkreślić przy tym należy, iż ich realizacja nie zależy wyłącznie od informatyków. W wymienionych dziedzinach niezbędna jest ścisła współpraca z logistykami oraz decydentami (a nawet politykami). W wielu sprawach konieczne będzie u nas przeprowadzenie odpowiednich badań i prac rozpoznawczych, we współpracy z doświadczonymi partnerami krajów Europy Zachodniej, a także szkoleń, zgodnie z zaproponowanymi przez nich programami edukacyjnymi.

Tylko kompleksowe podejście do problematyki budowy systemów logistycznych może dać oczekiwane efekty, czego potwierdzeniem są już przeprowadzone próby wdrożeń w przemyśle przetwórczym (owocowo-warzywnym), jako w jednym z ogniw łańcuchów logistycznych. Informatycy nie mogą pozostać bez odpowiedzi na to wezwanie nowoczesności.

LITERATURA

[1] Abt S.: Komputeryzacja handlu i przemysłu z zastosowaniem kodów kreskowych. INFORMATYKA nr 12'1991

[2] Abt S.: Aktualne i przyszłe wymogi eurologistyki wobec Polski. IGM, Poznań 1993 (maszynopis)

[3] Abt S., Woźniak H.: Podstawy logistyki. Uniwersytet Gdański, 1993

[4] Guide to Logistics Software 1993. Andersen Consulting.

ThinkPad z rzutnikiem i pisakiem

IBM rozpoczął produkcję nowych modeli notebooków z serii ThinkPad. W modelu 755CV zastosowano pomysłowe rozwiązanie monitora. Zdejmowany panel daje możliwość połączenia komputera z różnymi typami rzutników. Po odsłonięciu tylnego modułu, obrazy na ekranie komputera stają się przezroczystymi slajdami, które można rzucić na ścianę lub ekran za pomocą lampy projektora. Notebook ten jest też wyposażony w urządzenie do zdalnej kontroli w podczerwieni, z możliwością wykorzystania 22 efektów specjalnych, takich jak np. powiększanie wybranego fragmentu czy podświetlenie. Model – ThinkPad 755CX jest pierwszym komputerem przenośnym wyposażonym w Pentium z zegarem 75 MHz, pamięć podręczną L2 o pojemności 25 KB, baterię litową i monitor SVGA o rozdzielczości 800 × 600. Atrakcją ThinkPad 370C jest kolorowy monitor ciekłokrystaliczny (TFT) o przekątnej 10,4 cala, natomiast ThinkPad 360PE to udoskonalona wersja składanego notebooka 360P z kartą dźwiękową i pisakiem. Dzięki specjalnej konstrukcji monitora można go nałożyć na klawiaturę, uzyskując w ten sposób ekran stanowiący swoistą powierzchnię notatnika, na którym można zapisywać informacje bez używania klawiatury.

Homologacja systemów informatycznych

Zdzisław Szyjewski
Uniwersytet Szczeciński

Naturalną jest sytuacja, że każdy nowy pojazd, który ma uczestniczyć w ruchu drogowym, musi spełniać określone wymagania techniczne i eksploatacyjne. Wymagania te obowiązują producenta nowych pojazdów oraz użytkownika pojazdu w czasie eksploatacji. Procedura sprawdzenia zgodności z ustanowionymi wymaganiami polega na wykonaniu badań i formalnym dopuszczeniu lub niedopuszczeniu pojazdu do udziału w ruchu drogowym. Procedura ta nazywa się homologacją pojazdu.

Podstawowym założeniem procedury homologacji pojazdu jest zapewnienie bezpieczeństwa wszystkim użytkownikom ruchu drogowego. Odstępstwo od wyznaczonych norm może zagrażać nie tylko bezpośredniemu użytkownikowi pojazdu, ale również innym uczestnikom ruchu drogowego. Bezpieczeństwo użytkownikom mają gwarantować zasady ruchu drogowego oraz sprawność techniczna pojazdu. Sprawność techniczna jest oceniana na podstawie zgodności z ogólnymi zasadami (liczba i rodzaj świateł, minimalne wyposażenie dodatkowe itp.) oraz badania niektórych parametrów eksploatacyjnych pojazdu (siła hamowania, czystość spalin itp.).

Homologacja nowych pojazdów spoczywa na producencie, który ma obowiązek używać homologowanych części oraz określonych procedur i urządzeń wytwarzania. Wymagania stawiane producentowi nie są definiowane szczegółowo, a dotyczą tylko newralgicznych dla produktu końcowego części i procedur produkcji. Nowy model czy typ pojazdu otrzymuje certyfikat homologacyjny po pozytywnym odbyciu trudnych i złożonych badań i prób.

Procedura homologacji pojazdu wykształtowała się w wyniku wielu lat doświadczeń publicznego ruchu drogowego i dla dobra wszystkich jego użytkowników jest konsekwentnie przestrzegana i stale doskonalona. Odstępstwa od tych zasad są możliwe jedynie w przypadku, gdy pojazd użytkowany jest lokalnie i nie uczestniczy w publicznym ruchu drogowym.

To długie wyjaśnianie zasad homologowania pojazdów wynika z dużego podobieństwa sytuacji użytkowania pojazdów i użytkowania systemów informatycznych. Historia zastosowań informatyki jest znacznie krótsza niż historia motoryzacji, ale wpływ na życie codzienne jest podobny. Rewolucyjność zmian spowodowanych stosowaniem komputera jest podobna do zmian spowodowanych rozwojem motoryzacji. Należy spodziewać się, że problemy porządkowania zasad dopuszczania do użytkowania oraz organizacja użytkowania w publicznych sieciach informatycznych systemów informatycznych, będą podobne. W celu uniknięcia błędów warto skorzystać z doświadczeń motoryzacji i adaptować niektóre procedury na grunt informatyki.

Liczba komputerów oraz dziedziny życia, w których systemy informatyczne są stosowane powodują, że należy zająć się porządkowaniem procedur organizacyjnych regulujących dopuszczenie do użytkowania i kontrolą procesu eksploatacji. Możliwe do wystąpienia zagrożenia wynikające z korzystania z niesprawnych systemów informatycznych stają się coraz bardziej realne i to powinno zmusić wszystkich użytkowników systemów informatycznych do wypracowania zasad podobnych do stosowanych w ruchu drogowym.

Systemy informatyczne stosowane w tzw. systemach krytycznych typu badania jądrowe, loty kosmiczne itp. podlegają odpowiedniej procedurze badania jakości. Badania te mają gwarantować wysoki stopień bezpieczeństwa użytkowania systemów informatycznych. Procedury te są bardzo sformalizowane i nie mają bezpośredniego przeniesienia na inne systemy informatyczne, gdzie ewentualna awaria ma mniej groźne skutki lub zasięg ich oddziaływania jest mniejszy.

Bezpieczeństwo użytkowania systemu informatycznego w służbie zdrowia czy bankowości jest porównywalne z problemami występującymi w systemach krytycznych. Prowadzi to do wniosku, że coraz szersze stosowanie systemów informatycznych w różnych dziedzinach działalności zmusza do wypracowania metod gwarantujących bezpieczeństwo ich użytkowania. Powinny to być ogólne zasady i wytyczne gwarantujące niedoświadczonemu użytkownikowi minimum bezpieczeństwa. Wypracowanie norm oraz procedur homologowania systemu informatyczngo staje się koniecznością.

Systemy informatyczne są stosowane w coraz bardziej newralgicznych działach życia gospodarczego. Wmontowanie systemów informatycznych w procedury działalności gospodarczej powoduje uzależnienie gospodarki od sprawności i jakości systemów informatycznych. W pierwszej kolejności należałoby wypracować procedurę homologowania systemów wykorzystywanych w działalności finansowo-księgowej. Mnogość systemów finansowo-księgowych na rynku, w połączeniu z nie najwyższą jakością niektórych z nich, powoduje znaczne zagrożenie bezpieczeństwa informacji. Duże nakłady poniesione na sprzęt komputerowy w połączeniu z nietrafionym zakupem systemu informatycznego, zastosowanego w newralgicznej dla każdego przedsiębiorstwa działalności księgowej, są nie tylko nietrafioną inwestycją, ale powodują wymierne straty finansowe i złą atmosferę wokół informatyki. W interesie użytkownika i informatyków jest stworzenie mechanizmów eliminowania takich systemów informatycznych z rynku.

Należy stworzyć mechanizmy gwarantujące kupującemu minimum bezpieczeństwa przy wdrożeniu systemu informatycznego do działalności gospodarczej. Ryzyko handlowe związane z zakupem może dotyczć niektó-

rych cech jakościowych, solidności sprzedawcy w zakresie świadczonych usług dodatkowych i serwisu, ale wdrożony system nie może zagrażać funkcjonowaniu przedsiębiorstwa wskutek dezinformowania kierownictwa w dziedzinie stosowania systemu. Niewykluczone jest również wprowadzanie błędów w obszarach współpracy własnego przedsiębiorstwa lub w innych przedsiębiorstwach, z którymi system ma połączenia informatyczne.

Procedura homologacji

Działalność homologacyjna wymusza wprowadzenie niezbędnej biurokracji związanej z procedurą sprawdzania zgodności z wymaganiami. Każda biurokracja zmusza do sformalizowania procedur i tworzenia niezbędnej dokumentacji. Działania te będą niewątpliwie uciążliwe dla informatyków, którzy nigdy nie lubili dokumentować swoich prac, ale wymuszą opracowanie dokumentacji systemu i to według jednolitej metodyki. Będzie to dodatkowa korzyść z wprowadzenia procedur homologacji. Standard dokumentacji na potrzeby homologacji może stanowić zaczyn porządkowania problemów metodycznych, które od dawna wymagają unormowania. Prezentacja systemów na różnorodnych imprezach informatycznych czy nieliczne jeszcze przetargi na systemy informatyczne pokazują, że brakuje standardu niezbędnego minimum dokumentacyjnego. Brak dobrej dokumentacji nie jest tylko usterką techniczną, ale może być znacznym utrudnieniem w prawidłowej ocenie jakości systemu. Nieporównywalność dokumentacji jest równoznaczna z brakiem możliwości porównania systemów, co utrudnia podejmowanie decyzji wyboru produktu. Brak możliwości jednoznacznej oceny zwykle premiuje produkty słabszej jakości.

Samodzielnym problemem staje się definicja wymagań, jakie system informatyczny powinien spełniać. Wymagania te powinny dotyczyć niezbędnego minimum bez wnikania w szczegółowe metody realizacji, które mogą stanowić tajemnicę handlową producenta. Specyfika wymagań może więc dotyczyć jedynie oznak zewnętrznych funkcjonowania systemu, a nie szczegółowych rozwiązań informatycznych.

Wymagania te powinny być zgrupowane w trzy działy tematyczne:
- organizacyjno-prawne,
- merytoryczne,
- technologii informatycznej.

Wymagania organizacyjno-prawne

Wymagania organizacyjno-prawne powinny określać, jakie uwarunkowania organizacji prac systemu informatycznego muszą być zgodne z przepisami ogólnymi. Rozwiązania systemu informatycznego muszą być zgodne z obowiązującym prawem regulującym daną dziedzinę działalności. Wymagania te będą różne dla różnych klas systemów informatycznych. Ta grupa wymagań powinna być opracowywana odrębnie dla każdej klasy systemu i w sposób ciągły modyfikowana w miarę wprowadzania nowych uregulowań prawnych.

Wymogiem prawnym powinna być konieczność używania przez producenta systemu informatycznego tylko licencjonowanego oprogramowania operacyjnego i narzędziowego, wykorzystywanego przy produkcji oprogramowania. System otrzymujący certyfikat homologacji staje się równocześnie prawnie chroniony. Procedura homologacji będzie również sprzyjała standaryzacji rozwiązań organizacyjnych i prawnych nie tylko w informatyce, ale również w dziedzinach stosowania homologowanych systemów.

Wymagania merytoryczne

Wymagania merytoryczne określają podstawowe zasady, jakie musi spełniać algorytm realizowany przez system informatyczny. Określenie zasadniczych ram funkcjonalnych nie ogranicza inwencji autorów rozwiązań, a jedynie reguluje oznaki zewnętrzne funkcjonowania systemu. W przypadku systemu finansowo-księgowego są to zasady księgowania i prowadzenie ewidencji księgowej przez system informatyczny tak, aby zapisy tworzone i przechowywane w systemie gwarantowały możliwość kontroli oraz uzyskania niezbędnej wymaganej przepisami statystyki. Wymogi te powinny być uzgodnione z odpowiedzialnymi jednostkami administracji państwowej i stowarzyszeniami branżowymi.

Wymagania technologii informatycznej

Wymagania z zakresu technologii informatycznej powinny koncentrować się na problemach bezpieczeństwa informacji. Bezpieczne powinny być dane konkretnego systemu, ale równocześnie istotne jest, aby w przypadku jego błędnego funkcjonowania nie powodował awarii w otoczeniu informatycznym. Problem jest szczególnie groźny w przypadku systemów użytkowanych w sieciach komputerowych. Im szerszy zasięg sieci, tym ostrzejsze powinny być wymagania ochronne.

Procedura testowania systemów jest najczęściej opracowywana przez producenta, co nie gwarantuje wykrycia wszystkich usterek. Opracowanie standardowych testów przez niezależny zespół ekspertów może w istotny sposób wpłynąć na jakość oprogramowania systemów. Testowanie w sytuacjach krańcowych zapobiegnie awariom występującym długo po rozpoczęciu eksploatacji i w okresie gwarancji producenta. Działania te będą chronić użytkownika systemu przed niesolidnością producenta oraz groźnymi dla funkcjonowania przedsiębiorstwa usterkami systemów informatycznych.

Administrowanie procedurą homologacji

Na potrzeby homologacji powinny powstać niezbędne dokumenty homologacyjne, z których pierwszym i najistotniejszym powinien być zbiór wymagań opracowany odrębnie na potrzeby każdej homologowanej klasy systemów informatycznych. Dokument udostępniany producentom systemów informatycznych powinien stanowić pierwszy krok procedury homologacji. Dokument ten w swej podstawowej wersji powinien być stały, ale w miarę wprowadzania nowych uregulowań prawnych, czy wdrażania nowych technologii, powinien być na bieżąco modyfikowany. Z uwagi na powszechność stosowania systemów informatycznych w działalności finansowo-księgowej właśnie ta klasa systemów powinna być pierwszą, która może wprowadzić procedurę homologacji. Algorytmy finansowo-księgowe są najlepiej zdefiniowane, a skutki złej jakości systemów informatycznych mogą mieć najgroźniejsze konsekwencje.

Prowadzenie procedury homologacji wymaga odpowiedniej organizacji administracji obsługującej cały proces. Administracja powinna obejmować swym zasięgiem cały kraj i mieć możliwości techniczne prowadzenia aktualnej kartoteki systemów, które zostały dopuszczone do użytkowania oraz tych, które rozpoczęły procedurę homologacji i są w jej trakcie. Wzorce oprogramowania systemów, które otrzymały homologacje, muszą być

stale przechowywane i stanowią jedyny dokument, który będzie podstawą rozstrzygania wszelkich reklamacji i uwag użytkowników.

Wzorcowe oprogramowanie, zdeponowane w trakcie procedury homologacyjnej, chroni producenta przed nieautoryzowanym wprowadzaniem zmian i modyfikacji do systemu. Rozstrzyganie sporów między producentem oprogramowania a użytkownikiem po pewnym okresie eksploatacji jest bardzo uciążliwe bez posiadania zdeponowanego wzorca oprogramowania. Wzorcowe oprogramowanie staje się równocześnie gwarancją dla użytkownika, że wszelkie wady ukryte, które dały o sobie znać po okresie gwarancji, muszą być przez producenta usunięte.

Baza danych systemów homologowanych wymaga utrzymania i powinna umożliwiać łatwe homologowanie nowych wersji systemu już homologowanego. Biura administrujące procedurę homologacji powinny być wspomagane zespołami specjalistów wysokiej klasy, którzy będą gwarantować wysoką jakość ocen merytorycznych w kategoriach wymienionych wcześniej.

System stopni specjalizacyjnych w informatyce jest działaniem komplementarnym homologacji systemów informatycznych. Polskie Towarzystwo Informatyczne, inicjator stopni specjalizacyjnych, powinno rozszerzyć zasięg normalizacji na systemy informatyczne. Należy pamiętać o współpracy Towarzystwa z prawnikami w trakcie początkowych prac nad ochroną praw autorskich oprogramowania. Aktywna współpraca ze stowarzyszeniami branżowymi może doprowadzić do wykształtowania się zespołów interdyscyplinarnych, posiadających niezbędną wiedzę i kwalifikacje dla obsługi procedury homologacji. Pozostaje jedynie stworzenie odpowiedniej infrastruktury administracyjnej i technicznej dla obsługi tego procesu.

Działalność homologacyjna powinna mieć odpowiednią rangę akceptowaną przez administrację państwową. Rola administracji państwowej powinna być wyraźnie określona, ale przede wszystkim należy dbać o wagę merytoryczną procedury. Urzędnicy mają zawsze skłonność do zbiurokratyzowania każdej procedury, co często prowadzi do zaniku podstawowej idei. Rola administracji w procesie homologacji powinna więc ograniczać się do działań czysto administracyjnych. Osiągnięcie takiej pozycji będzie możliwe tylko wtedy, gdy dominująca stanie się procedura merytoryczna.

Certyfikat homologacji powinien stanowić dokument państwowy o odpowiedniej wadze. Podpisany przez zespół merytoryczny certyfikat taki będzie gwarantem odpowiedniej jakości produktu, a urzędowa pieczęć administracji państwowej nada mu rangę zgodnie z procedurą administracyjną. Wdrożenie certyfikatu homologacyjnego uprości obrót oprogramowania i wprowadzi mechanizmy porządkowania zastosowań systemów informatycznych w różnych dziedzinach działalności.

Procedura homologacji będzie promować systemy wysokiej jakości, a przez certyfikat będzie wdrażać znak jakości rozwiązań informatycznych. Pozwoli to na promowanie rozwiązań zgodnych z ogólnymi założeniami polityki państwa. Łatwiejsze stanie się wdrożenie nowych rozwiązań kierunkowych związanych z realizacją umów międzynarodowych czy restrukturyzacją całych gałęzi gospodarki.

Artykuł był prezentowany na Szóstej Międzynarodowej Górskiej Szkole PTI w Szczyrku, w dniach 20–24 czerwca 1994 r.

Prosto z firm ● Prosto z firm ● Prosto z firm ● Prosto z firm

„THE ROCARELLI REport of Computer Animation" za 1994 r. podaje, iż pakiet **3D Studio** firmy Autodesk umocnił swoją pozycję wśród profesjonalnych aplikacji do animacji 3D: jego udział na tym rynku wzrósł z 31% do 48%. Z badania rynku oprogramowania animacyjnego (na świecie pracuje ponad 100 tys. stanowisk animacyjnych) dla platform PC, Macintosh i Silicon Graphics wynika, że 3D Studio stanowi aż 75% oprogramowania wykorzystywanego na PC (50% przed dwoma laty). 3D Studio otrzymało też wiele znaczących nagród przyznawanych przez pisma poświęcone m.in. animacji, grafice komputerowej, multimediom i automatyzacji projektowania.

*

DOTYCHCZASOWA dystrybucja sprzętu firmy Zenith Data Systems w Polsce organizowana była na zasadach współpracy z wieloma *resellerami*. Od maja dystrybutorem sprzętu ZDS jest warszawska firma Lumena. W ofercie są *notebooki*, stacje robocze z magistralą PCI, stacje graficzne, a od czerwca nowa rodzina serwerów z magistralą PCI–EISA, certyfikowanych przez Novella i SCO Unix. Zawarta w maju br. umowa daje Lumenie wyłączność na *notebooki*.

*

JTT COMPUTER ZAwarł umowę dystrybucyjną z firmą **Groupe Schneider**, co sprawia, że powiększa swoją ofertę o zasilacze francuskiego producenta – Merlin Gerin. Mogą być one zarządzane przez sieci LAN i WAN. Do tego celu jest wykorzystywany UM-Link, czyli adapter SNMP oraz oprogramowanie pozwalające na współpracę ze wszystkimi pracującymi w Polsce systemami operacyjnymi. Merlin Gerin uzyskał certyfikat zgodności ze standardami IETF dla swojego UPS MIB (*Management Information Base*).

*

5 CZERWCA BR. ROZpoczęła się publiczna subskrypcja akcji ComputerLandu. W ofercie publicznej zaoferowano 390 720 akcji serii „E", które sprzedawano po 22,50 zł w pakietach po 10 akcji. ComputerLand powstał ponad 4 lata temu. Założycielami była szwedzka firma UIS International i Ryszard Krauze. Po kilku miesiącach udziałowcem został Tomasz Sielicki, prezes zarządu ComputerLand Poland, który tę funkcję pełni nieprzerwanie od 1991 r. Obroty spółki w 1994 r. osiągnęły poziom 600 mld zł, ComputerLand jest na 290 miejscu na prezentowanej przez „Gazetę Bankową" liście 500 największych polskich przedsiębiorstw.

*

COMPUTER 2000 – NAJwiększy europejski dystrybutor sprzętu i oprogramowania – poinformował, iż w I kwartale nowego roku finansowego (rozpoczął się w październiku 1994 r.) sprzedaż całej grupy wyniosła 1,3 mld DEM, co oznacza wzrost o 41,2% w porównaniu z I kw. poprzedniego roku finansowego. Największy wzrost – 60% – nastąpił w Europie północnej i południowej, w Europie środkowej wyniósł on 14%. W Polsce przedstawicielem grupy jest firma C2000 Polska (dawniej DHI), której obroty w 1994 r. przekroczyły 882 mld zł (ok. 38 mln USD).

*

FIRMA HEWLETT-PAckard została wybrana na oficjalnego dostawcę technologii informatycznej na potrzeby mistrzostw świata w piłce nożnej w 1998 r. HP liczy, że przysporzy to jej nowych, licznych klientów. Firma ogłosiła wyniki I półrocza roku finansowego, który zakończył się 30 kwietnia br. Zysk netto wyniósł 1,2 mld USD – co oznacza wzrost o 52% w porównaniu z pierwszym półroczem ub.r. Zamówienia ukształtowały się na poziomie 15,8 mld USD, z tego w USA – 6,6 mld USD. Zysk netto w przeliczeniu na jedną akcję wzrósł o 51%.

*

MINISTERSTWO EDUkacji Narodowej zawarło kontrakt z firmą Microsoft Polska na dostawę oprogramowania. Do naszych szkół trafiło 4000 licencji na MS-Works. Uczniowie otrzymali więc standardowy zestaw programów, jakie są najczęściej używane w pracy z komputerem. Jednolitość oprogramowania stwarza nauczycielom możliwość wymiany doświadczeń.

(kar.)

Prosto z firm ● Prosto z firm ● Prosto z firm ● Prosto z firm

Perspektywy rozwoju rynku komputerów osobistych

Robert Repeć
Instytut Informatyki Teoretycznej
i Stosowanej PAN
Gliwice

Stały rozwój istniejącego rynku personalnego sprzętu komputerowego oraz wymagań użytkowników nie pozwala producentom oprogramowania na lenistwo. Pojawienie się 32-bitowych procesorów takich, jak Intel i386 czy Motorola 680xx spowodowało zaistnienie silnego trendu wymuszającego tworzenie nowych programów, a dokładniej systemów operacyjnych wykorzystujących jak najlepiej powstałe możliwości. Wykorzystanie całej przestrzeni adresowej, płaski model pamięci, wbudowane mechanizmy sieciowe to tylko niektóre potrzeby dzisiejszego rynku.

Nowe procesory w połączeniu z coraz ciekawszymi koncepcjami, takimi jak Plug & Play, czy PCMCIA, powiększają moc obliczeniową i użytkową komputera osobistego odciążając tym samym „duże" systemy komputerowe. Użytkownik może zatem zaoszczędzić więcej czasu i pieniędzy, co zwykle zwiększa jego zadowolenie. Interesujące będzie krótkie scharakteryzowanie wspomnianych „ciekawych koncepcji" w rozwoju sprzętu personalnego.

Tendencje rozwoju sprzętu

Na wstępie kilka słów na temat nowinek technicznych i kierunków rozwoju rynku komputerów osobistych.

Miniaturyzacja i łączność (modem, LAN, WAN)

Od pewnego czasu silnie rysuje się koncepcja „biura w domu", która polega na zdalnym dostępie do zasobów biurowych, czy to przez sieć WAN, czy modem. Jest to domena szczególnie dziennikarzy korespondencyjnych i pracowników środowiskowych. Dla tych przede wszystkim zawodów powstały takie rodzaje komputerów osobistych, jak laptop czy notebook. Nie należy też zapominać o biznesmenach i kontrolerach (np. inkasent gazowni), którzy dla swoich zastosowań mogą korzystać z maszyn typu *palmtop*, czy PDA (*Personal Data Assistant*).

Wzrost mocy obliczeniowej

Naturalnym dążeniem człowieka posiadającego komputer jest stałe zwiększanie szybkości jego obliczeń kontrolowanych bądź przez pomiar odczuć subiektywnych, bądź użycie programów typu *benchmark*. Producenci sprzętu, znając te problemy, wychodzą naprzeciw oczekiwaniom przez produkcję coraz szybciej taktowanych procesorów lub uwzględnianie programów testowych w mikroprogramach produktu (dotyczy szczególnie kart graficznych). Jednak głównym problemem, nurtującym obecnie użytkowników komputerów jest wybór między:

- linią tradycyjną (CISC): Intel i386, i486, Pentium;
- redukcją listy rozkazów (RISC): Alpha, MIPS, PowerPC

Nie sposób przewidzieć, w którym kierunku potoczy się ostatecznie świat, więc jak dotąd wybór jest raczej losowy.

Wzrost inteligencji podzespołów

Dążenie do zwiększenia energooszczędności komputerów, zwiększenia współczynnika „idiotoodporności" i uproszczenia zmian konfiguracji zaowocowało powstaniem:

- ***Power Management*** **(EPA)**

Koncepcja, sygnowana zwykle znakiem EPA *Pollution Preventer*, umożliwia zmniejszanie całkowitego poboru mocy przez sterowanie poszczególnymi elementami systemu komputerowego: procesorem, dyskami i monitorem;

- **nowych koncepcji magistral i złącz**

Magistrala ISA (16 bitów) komputera IBM nie wystarcza już dla obecnych zastosowań, a powstała jakiś czas temu 32-bitowa EISA nie jest rozwiązaniem tanim, powstały zatem nowe rozszerzenia:

  - □ **32-bitowy VESA Local Bus (projektowany 64-bitowy Local BUS II)**

    Dodatkowe złącze, dające możliwość szybkiej transmisji jednak najwyżej tylko dla trzech urządzeń. Charakter transmisji powoduje, że dla większej liczby uczestników transmisji wydajność jest mniejsza niż bez Local Bus;
  - □ **32-64-bitowa magistrala PCI**

    PCI jest rozwiązaniem, które pozwala na osiągnięcie bardzo dużej szybkości transmisji danych, bez ograniczenia do trzech urządzeń. Magistrala jest 32 lub 64-bitowa w zależności od typu procesora.

Łatwość konfiguracji komputera jest wspomagana przez stosunkowo nową koncepcję złącza zewnętrznego

Mgr inż. ROBERT KRZYSZTOF REPEĆ w 1993 r. ukończył Wydział Automatyki, Elektroniki i Informatyki Politechniki Śląskiej w Gliwicach na kierunku Informatyka. Obecnie pracuje w Instytucie Informatyki Teoretycznej i Stosowanej PAN w Gliwicach. Zajmuje się heterogenicznymi sieciami komputerowymi.

PCMCIA (I, II lub III) pozwalającą na przyłączanie takich urządzeń jak modem – fax, dysk twardy, pamięć (FLASH RAM/HDD) zgodnie z pomysłem „podłącz i używaj", czyli Plug & Play.

■ **Plug & Play**

Pomysł ten, stanowiący zrealizowane marzenie pokoleń użytkowników komputerów umożliwia zastąpienie w trakcie działania komputera modemu twardym dyskiem, bez ryzyka uszkodzenia i potrzeby restartu. Plug & Play pozwala na rozpoznanie urządzenia automatycznie, bezpośrednio po przyłączeniu do komputera.

Rozwój pamięci masowych

Wzrost szybkości komputerów idzie w parze z wysiłkami programistów, którzy tworzą coraz większe objętościowo programy. Jeśli spojrzeć w przeszłość, to parę lat temu dysk rzędu 100 MB był wystarczający do bardzo dużej gamy zastosowań. Ostatnie lata rozwoju systemów graficznych spowodowały jednak, że 100 MB ledwo wystarcza na zainstalowanie dobrego edytora tekstów, arkusza kalkulacyjnego i programu graficznego typu CorelDraw w podstawowej konfiguracji.

■ **Sterowniki IDE**

Sterowniki typu IDE są od dawna bardzo popularnym rozwiązaniem, które pozwala na przyłączenie dwóch urządzeń (HDD lub IDE CD-ROM) do jednego sterownika. W porównaniu z interfejsami SCSI jest o wiele tańsze i sprawiające mniej kłopotów, osiągając obecnie zarówno porównywalne pojemności dysków (do ok. 500 MB) jak i szybkości, szczególnie po opracowaniu standardu Enhanced. W komputerach PC pojemności dysków IDE mogą osiągnąć ok. 8 GB w tak zwanym trybie LBA (*Logical Block Address*), zapewnianym przez płytę główną, bądź sterownik E-IDE.

■ **Enhanced IDE**

Rozwiązanie to nie wymaga żadnych istotnych zmian konfiguracji, poza dyskiem i sterownikiem akceptującymi standard poszerzony. Należy zaznaczyć, że zarówno dysk, jak i sterownik mogą pracować w „zwykłym" IDE. Korzyścią z zmiany jest zwykle zarówno możliwość przyłączenia do czterech urządzeń IDE/E-IDE, jak i wzrost prędkości przesyłania danych do ok. 11 MB/s!

■ **WORM/CD-ROM/dysk MO**

Po próbach stosowania przez rzesze użytkowników pamięci taśmowych, na pierwsze miejsce pod względem popularności wysuwają się dyski optyczne CD-ROM. Są one wolniejsze od przeciętnych dysków twardych, a najszybsze (*quadruple speed*) osiągają pułap szybkości przesyłu danych zaledwie ok. 600 kB/s. Dyski magnetooptyczne (MO) mając przewagę możliwością wielokrotnego zapisu informacji są niedostępne dla przeciętnego posiadacza komputera ze względu na kilkunastokrotną różnicę w cenie w stosunku do CD-ROM. Duża pojemność magazynowanej informacji oraz przyzwoity czas jej udostępniania predestynują dyski optyczne do zastosowań archiwizacyjnych, a przede wszystkim multimedialnych.

Po tym krótkim wyliczeniu nowości w dziedzinie sprzętowej, które obecnie fascynują świat, należy wymienić wymagania dotyczące oprogramowania.

Wymagania dotyczące nowych systemów operacyjnych

Jaki powinien być nowoczesny system operacyjny? Co powinien oferować i czego żądać od użytkownika? Przede wszystkim:

■ **Wieloprocesowość**

Bardzoa ważna obecnie właściwość systemu operacyjnego. Pozwala na jednoczesne bądź przynajmniej symulowane jednoczesne działanie wielu procesów użytkowych. Systemy takie jak DOS, z jego programami rezydentnymi, które nie mają żadnych mechanizmów obsługi wieloprocesowości, odchodzą powoli w zapomnienie. Obecnie użytkownik żąda od systemu zapewnienia **bezpiecznej** możliwości użycia kilku programów, które przynajmniej rezydują w pamięci w tym samym czasie. Mechanizm TSR (*Terminate and Stay Resident*) oraz wywoływania procesora komend z wnętrza innego programu są w obecnej postaci zbyt niebezpieczne i wymagają rzetelnego przygotowania dla potrzeb wieloprocesowości.

■ **Wielowątkowość**

System wieloprocesowy może zapewniać mechanizmy umożliwiające rozdział procesu wykonywanego na niezależnie działające podprocesy nie wymagające przydziału osobnego środowiska. Takie podprocesy są nazywane wątkami (ang. *threads*). Jest to bardzo cenna właściwość systemu, umożliwiająca rzeczywiste przyspieszenie działania **jednego** procesu.

■ **Wysoki stopień bezpieczeństwa danych i odporności systemu**

Użytkownik komputera jest człowiekiem, którego może prześladować pech psujących się urządzeń lub brak odpowiednich umiejętności. W takiej sytuacji odporny system operacyjny jest na wagę złota! Oparcie się dłonią o klawiaturę nie powinno demolować całego systemu, a błędny sektor na dysku nie może odcinać dostępu do kilkuset megabajtów danych, które pracowicie trzeba będzie wprowadzić na nowo. Dlatego właśnie tak ważne są podane dalej mechanizmy systemowe:

□ **Poziomy dostępu**

Żaden użytkownik nie jest nieomylny, dlatego optymalne rozdzielenie praw użytkowania newralgicznych narzędzi systemowych jest bardzo istotne w prawidłowym użytkowaniu systemu. Zapomnienie jednego hasła nie może powodować bezpowrotnego utracenia dostępu do danych, ale z drugiej strony jeden klucz nie może otwierać wszystkich drzwi!

□ **Odtwarzanie utraconych danych**

Uszkodzona dyskietka, gapiostwo przy wprowadzaniu polecenia usuwania pliku nie są rzeczami unikalnymi. Dobry system powinien dysponować narzędziami umożliwiającymi przynajmniej próbę odtworzenia danych.

□ **Mechanizmy bezpieczeństwa sieciowego**

Zdalny dostęp do zasobów maszyny jest rzeczą ułatwiającą integrację biura, czy zakładu w jedną sprawnie działającą sieć lub umożliwiającą udostępnienie szerszemu ogółowi wyników własnych prac. Nie należy jednak zapominać, że konieczne jest zarządzanie zasobami w celu uniknięcia bałaganu, a co ważniejsze, nieautoryzowanego dostępu, który może być po prostu kradzieżą.

■ **Pełne wykorzystanie istniejących zasobów**

Kupując komputer użytkownik pragnie wykorzystać go w stopniu maksymalnym. Systemy, które rezerwują olbrzymie obszary drogiej pamięci do bliżej niesprecyzowanych celów, lub nie mogące wykorzystać całości dostępnej przestrzeni dyskowej czasami tylko irytują, ale często utrudniają bądź uniemożliwiają pracę. Nowoczesny system operacyjny powinien korzystać z zasobów komputera w sposób optymalny.

□ **Pamięć**

Ta część komputera jest nadal bardzo kosztowna, mimo marzeń użytkowników, dlatego mile widziane są systemy, które potrafią zrobić jak najwięcej, przy jak najmniejszej pamięci.

□ **Dyski (kompresja danych w locie)**

Wolnej przestrzeni dysku nigdy za wiele i stąd wynikły próby stworzenia systemów kompresujących dane w locie. Duże rysunki, pliki dźwięków, teksty są zwykle łatwe do kompresji, a więc system powinien przynajmniej niektóre kompresje wykonywać automatycznie.

□ **Grafika (rozdzielczość, kolor)**

Oczywiście nie każdy użytkownik jest grafikiem, który potrzebuje ponad 16 milionów kolorów, ale w systemach operacyjnych zawierających interfejs graficzny (GUI), duże rozdzielczości ekranu i przyzwoite kilka tysięcy kolorów są mile widziane.

□ **Dźwięk**

Uzupełnienie informacji wizualnej dźwiękiem jest oczywistym ułatwieniem i uatrakcyjnieniem walorów systemu operacyjnego. Nie należy przy tym zapominać o możliwości sterowania dźwiękowego oraz syntezy mowy. Rozmawiający, w sposób inteligentny, komputer jest przecież marzeniem twórców SF nie od wczoraj.

- **Niezależność sprzętowa, przenośność, skalowalność systemu**

Liczba rozmaitych platform sprzętowych produkowanych na świecie potrafi przyprawić o ból głowy, a nie ma przecież powodu, żeby dobry system nie działał zarówno na komputerze typu mainframe w miejscu zatrudnienia, jak i, być może w zmniejszonej wersji, na PC w domu... Nowo powstała koncepcja mikrojąder (ang. *microkernels*), gdzie jądro-rdzeń systemu ma rozmiary rzędu kilkunastu kilobajtów bardzo dobrze ilustruje realizację tego wymagania. System oparty na mikrojądrze jest niewielki w swej podstawowej wersji i pozwala na dołączanie specyficznych dla danej maszyny (ang. *site specific*) sterowników urządzeń zewnętrznych. Cała nadbudowa, powyżej warstwy sterowników, jest niezależna sprzętowo. Stąd wynika też potrzeba obiektowości i modularności systemu.

- **Modularność**

System operacyjny składający się z rdzenia i przyłączalnych modułów ma wiele zalet: jest łatwiejszy w tworzeniu i testowaniu, a także dostosowaniu do potrzeb użytkownika.

- **Obiektowość**

Obiekty stanowią odkrycie ostatnich lat, są związane z modularnością i pozwalają na łatwiejsze konstruowanie skalowalnych systemów operacyjnych o dużej niezależności od platformy sprzętowej. Mechanizmy OLE, OLE2 (*Object Linking and Embedding*), czy projektowany *OpenDoc* to również istotne usprawnienie funkcjonalności systemu.

- **Łatwość obsługi i modyfikacji (przyjazność)**

Ostatni, lecz nie najmniej ważny punkt! Przyjazny system operacyjny jest pożądany zarówno przez administratora, jak i szeregowego użytkownika. Prostota i intuicyjność obsługi jest istotną cechą ułatwiającą instalację i zarządzanie systemem, co pozwala, nawet mniej bezpiecznym systemom, osiągnąć poziom ich nawet bardziej idiotoodpornych krewniaków.

Charakterystyka niektórych 32-bitowych systemów operacyjnych

Należy teraz powiedzieć już nie tylko o pobożnych życzeniach użytkowników, ale ich realizacjach. Firmy Microsoft oraz IBM zrealizowały bądź wciąż próbują zrealizować marzenia olbrzymiej rzeszy posiadaczy współczesnych komputerów. Ich odpowiedzią są takie produkty, jak Windows NT Cairo, Chicago, WARP, UnixWare, QNX, Chorus/MiX, Interactive Unix 4.0, SCO Open Desktop, NeXTStep czy Solaris. Oto kilka zdań na temat niektórych z nich.

Windows NT 3.5 (Cairo)

Ostatnio prezentowany przez firmę Microsoft produkt stanowi zakończenie kolejnego etapu projektu Cairo. Jest to system z interfejsem graficznym, przewidziany do zdobycia rynku maszyn typu workstation, czyli szybkich, efektywnych komputerów o dużej przestrzeni pamięciowej i przyłączonych do sieci. Wersje NTServer i NTWorkstation są wyposażone w sieć *peer-to-peer* opartą na protokole *Net-BEUI*, przy czym NTServer jest projektowany jako serwer systemu plików o dużej efektywności, co pozwala na korzystanie również z zalet sieci typu *client-server*. Bardzo dobre mechanizmy bezpieczeństwa systemu plików, które zapewnia system NTFS (*New Technology File System*) oraz narzędzia kontrolujące poziomy dostępu ustawiają system Cairo w czołówce systemów operacyjnych. Oryginalna konstrukcja mikrojądra *NT Microkernel* powinna pozwolić na osiągnięcie dużej efektywności i skalowalności systemu.

Windows for Workgroups 4.0 (Chicago, Win95)

Ten graficzny system będący pośrednim pomiędzy Windows for Workgroups 3.11, a Windows NT Cairo powinien ukazać się już za kilka miesięcy. Nie wymagający tak dużej jak NT pamięci operacyjnej, pozbawiony chwiejnej podpory DOS-a, wyposażony w mechanizmy OLE (może SOM?), kompresję w locie, nowe formaty plików graficznych i zmienioną szatę graficzną, może się okazać nowym przebojem firmy Microsoft na rynku komputerów osobistych. Sieć *peer-to-peer*, w którą będzie wyposażony, pozwoli na połączenie biura w jedną całość, jak i przyłączenie do sieci Cairo.

OS/2 2.x i 3.0 WARP

Istniejący od dłuższego czasu produkt firmy IBM OS/2, którego wersja 2.0 została uhonorowana wyróżnieniem *PC Magazine Editors Choice*, ukazał się ostatnio w wersji 3.0. Wersja ta o nazwie *WARP* jest znakomitym systemem o bardzo dobrze widocznej obiektowości, którego dość ograniczone wymagania sprzętowe oraz duża paleta istniejących aplikacji być może pozwoli na wyprzedzenie konkurencyjnego produktu *Win95/Chicago* firmy Microsoft. System jest przyjazny, intuicyjny o szerokich możliwościach oraz dobrym poziomie bezpieczeństwa systemu plików HPFS. Możliwość uruchamiania aplikacji MB Windows (Standard i Enhanced) i MS DOS oraz bardzo dobra warstwa multimediów graficznego środowiska PM (*Program Manager*) z pewnością przyczynią się do wzrostu popularności OS/2.

Linux

W pełni funkcjonalny, publiczny (*public domain*) system operacyjny jest oparty na systemie UNIX i zawiera X Windows. Jego zaletami są małe wymagania sprzętowe, bogactwo dostępnych programów i dobry poziom bezpieczeństwa. Dostępne są emulacje MS DOS, możliwość obsługi popularnych kart dźwiękowych oraz czytników CD-ROM. Nowe wersje i poprawki pojawiają się jak grzyby po deszczu, więc dla użytkowników zalecany jest dostęp do sieci Internet.

dokończenie na s. 30

SYSTEMY CZASU RZECZYWISTEGO

REDAGUJE ZESPÓŁ: dr inż. Zbigniew FRYŹLEWICZ (Politechnika Wrocławska), prof. dr hab. inż. Janusz GÓRSKI (Francusko-Polska Wyższa Szkoła Nowych Technik Informatyczno-Komunikacyjnych w Poznaniu), prof. dr hab. inż. Zbigniew HUZAR (Politechnika Wrocławska), dr inż. Krzysztof SACHA (Politechnika Warszawska), prof. dr hab. inż. Tomasz SZMUC (Akademia Górniczo-Hutnicza), dr inż. Zbigniew ZIELIŃSKI (Wojskowa Akademia Techniczna), mgr inż. Zdzisław ŻURAKOWSKI (Instytut Automatyki Systemów Energetycznych we Wrocławiu) – przewodniczący zespołu.

ROK II ● LIPIEC ● 1995 ● 9

Niezawodność i bezpieczeństwo systemów komputerowych

Normy IEC dla systemów komputerowych związanych z bezpieczeństwem

Zdzisław Żurakowski
Instytut Automatyki Systemów Energetycznych Wrocław

Działalność normalizacyjna w dziedzinie wytwarzania i eksploatacji systemów komputerowych związanych z bezpieczeństwem rozpoczęła się w latach 70., jednak aktualny stan normalizacji w tej dziedzinie wciąż jeszcze nie jest dojrzały i wystarczający, przy czym główne trudności stwarza oprogramowanie. Do przyczyn takiego stanu rzeczy zaliczyć można:

- Sam charakter oprogramowania, które jest bardzo złożonym tworem intelektualnym, powstałym w procesie o charakterze w znacznym stopniu twórczym, i które w początkowym okresie było tworzone w sposób nieco podobny do twórczości artystycznej.
- Stan wiedzy i praktyki oraz posiadane w tej dziedzinie doświadczenie, które znajdują swoje odbicie w normach.

Obecnie nie istnieje ogólnie przyjęty konsensus dla wszystkich sektorów przemysłu, które stosują programowalne systemy elektroniczne związane z bezpieczeństwem. Każdy przemysł czy sektor przemysłu stosujący takie systemy ma już opracowane lub dopiero opracowuje normy dla swoich unikalnych potrzeb, patrząc na problem z własnej perspektywy. W niektórych przypadkach spotyka się nawet argumentację, że normalizacja w tej dziedzinie jest przedwczesna, że nie mamy jeszcze technologii ani doświadczeń odpowiednich do projektowania oprogramowania uwzględniającego specyfikę zastosowań związanych z bezpieczeństwem, które byłyby w stanie zapewnić akceptowalny poziom ryzyka [6]. W tej samej publikacji autorzy komentują tego typu poglądy stwierdzeniem, że argumenty takie nie powstrzymują jednak od opracowywania takich systemów i to dla zwiększającej się coraz szybciej liczby zastosowań.

Rosnące doświadczenie w projektowaniu tego typu systemów oraz tworzeniu i stosowaniu norm wraz z rosnącym stosowaniem metod inżynierii oprogramowania powodują, że normalizacja w rozważanej dziedzinie staje się łatwiejsza.

Z drugiej strony takie fakty, jak:

- możliwość jasnego i jednoznacznego porozumiewania się między wszystkimi zainteresowanymi stronami,
- możliwość odwoływania się do norm w kontraktach i prawodawstwie oraz ich używanie jako podstawy certyfikacji wyrobów i zarządzania jakością, a także zagwarantowanie nabywcom bezpieczeństwa produktów i usług opartych na oprogramowaniu,
- dostarczenie instrumentów przyczyniających się do rozwoju opartego na solidnych technicznych podstawach oraz do powstawania produktów bardziej uniwersalnych i spełniających wymagania handlu światowego,

przyczyniły się niewątpliwie do tego, że w krajach rozwiniętych w latach 80. zainteresowanie normalizacją w tej dziedzinie zaczęło rosnąć. Dotyczy to zarówno niektórych rządów, jak i użytkowników, przemysłu i organów regulujących te zagadnienia [5].

Należy również zauważyć, że o ile normalizacja zbyt wczesna może hamować rozwój danej dziedziny, to normalizacja spóźniona jest bezużyteczna zarówno dla dostawców, jak i dla użytkowników. Śledząc normalizację w rozpatrywanej dziedzinie można chyba stwierdzić, że rozwija się ona raczej zgodnie z wymaganiami rynku i rozwojem technologii. W znacznym stopniu potwierdzają to podane niżej fakty.

Działalność normalizacyjna IEC

Aktualnie istniejące na świecie normy można zgodnie z zakresem ich stosowania podzielić na sześć kategorii [5]:

- firmowe (w Polsce – zakładowe),
- branżowe,
- rządowe,

- uzgodnione (ang. *standard by consensus*), opracowywane przez przedstawicieli wszystkich sektorów zainteresowanych w korzystaniu z danej normy (np. ECMA, EWICS),
- wielonarodowe (CEN/CENELEC, NATON IAEA),
- międzynarodowe (IEC, ISO).

Normy międzynarodowe w dziedzinie technologii informatycznych są obecnie opracowywane przez IEC[1] oraz ISO[2]. Normy międzynarodowe odnoszące się do systemów komputerowych pełniących funkcje związane z bezpieczeństwem, opracowuje tylko IEC. IEC prowadzi ścisłą współpracę z ISO oraz z Europejskim Komitetem ds. Normalizacji Elektrotechnicznej (CENELEC), regionalną organizacją normalizacyjną założoną przez komitety elektrotechniczne organizacji normalizacyjnych państw członków Unii Europejskiej i EFTA. Polska jest krajem członkowskim IEC, a zainteresowane Komisje Polskiego Komitetu Normalizacji współpracują z odpowiednimi Komitetami Technicznymi IEC.

Bardzo istotnym wkładem krajów europejskich do prestandaryzacji w omawianej dziedzinie, stanowią prace organizacji EWICS (*Europe Workshop of Industrial Computer Systems*). Komitet TC7 tej organizacji, działający od 1974 r., zajmuje się zagadnieniami bezpieczeństwa (ang. *safety*), zabezpieczeń (ang. *security*) i niezawodności (ang. *reliability*) w dziedzinie systemów komputerowych czasu rzeczywistego przeznaczonego do zastosowań przemysłowych [5].

Efekty prowadzonej w latach 80. działalności normalizacyjnej w dziedzinie systemów komputerowych pełniących funkcje związane z bezpieczeństwem można scharakteryzować następująco [5]:

- W sektorze cywilnym na poziomie międzynarodowym najbardziej istotny wkład pochodził ze strony komitetu TC65 IEC;
- Wkładem europejskim, szczególnie komitetu TC7 EWICS, było przedstawienie propozycji, schematów, zasad, procedur i wytycznych instytucjom europejskim i międzynarodowym. Prace EWICS TC7 zostały szeroko przyswojone przez narodowe i międzynarodowe organizacje normalizacyjne. Przez swoich członków i swoje raporty komitet TC7 EWICS wywarł duży wpływ w międzynarodowych komitetach technicznych na proces normalizacji oprogramowania do zastosowań związanych z bezpieczeństwem;
- Działania normalizacyjne w omawianym zakresie podjęły także niektóre kraje europejskie. Najbardziej znane są wysiłki Wielkiej Brytanii (BSI), Niemiec (DIN) i Hiszpanii (AENOR). W niektórych krajach także powstała pewna liczba dokumentów z tej dziedziny, lecz są one ograniczone do poszczególnych dziedzin przemysłu lub mają ograniczony zakres stosowania do danego kraju;
- W sektorze militarnym różne normy i wytyczne USA służyły jako fundamentalne odniesienia. Również ostatnie publikacje w dziedzinie norm dla sektora militarnego w Wielkiej Brytanii (MoD), stanowią punkty odniesienia dla nowych, zaawansowanych norm w dziedzinie oprogramowania do zastosowań związanych z bezpieczeństwem.

Wszystkie opublikowane do chwili obecnej normy IEC dotyczące omawianego zakresu zagadnień oraz większość projektów norm zawiera załączony wykaz.

Dużą część istniejących norm z omawianego zakresu, zwłaszcza szerzej znanych, wymieniona jest w publikacjach [3, 5, 6], część z nich jest również omówiona.

W ostatnich latach szereg organów opublikowało lub opracowuje dalsze wytyczne umożliwiające bezpieczną eksploatację systemów komputerowych, nazywanych w anglojęzycznych publikacjach normalizacyjnych **elektronicznymi systemami programowalnymi** (*Programmable Electronic Systems* – PES). W Wielkiej Brytanii *Health and Safety Executive* opracował wytyczne dla systemów do zastosowań związanych z bezpieczeństwem[3]. W Niemczech został opublikowany projekt normy DIN[4]. We Wspólnocie Europejskiej, w ramach prac związanych z harmonizacją norm europejskich, są prowadzone prace z zakresu systemów związanych z bezpieczeństwem, w celu określenia dyrektywy dotyczącej maszyn (*Machinery Directive*). W USA *Instrument Society of America* (ISA) jest daleko zaawansowane w przygotowaniu normy dla PES stosowanych w przemyśle przetwórczym[5], *Center for Chemical Process Safety* oraz *Directorate of the American Institute of Chemical Engineers* przygotowuje wytyczne dla sektora chemicznego przemysłu przetwórczego[6] [1, 2].

Głównym nastawieniem wszystkich tych prac jest osiągnięcie normalizacji międzynarodowej [1, 2]. W związku z tym IEC opracowuje dwie normy międzynarodowe [8, 9], które mają być podstawową publikacją w zakresie bezpieczeństwa funkcjonalnego systemów związanych z bezpieczeństwem. Będą one miały niewątpliwie wpływ na wszystkie normy IEC dotyczące systemów związanych z bezpieczeństwem. Oczekuje się, że będzie to miało ważne konsekwencje dla tych wszystkich dziedzin przemysłu, w których systemy takie są stosowane i będzie prowadziło do wysokiego stopnia harmonizacji rozwiązań [1].

Projekty norm [8, 9] zostaną w artykule przedstawione bardziej szczegółowo.

Projekty norm międzynarodowych IEC

Pierwsze wersje projektów norm [8, 9] zostały rozesłane do komitetów narodowych krajów członkowskich IEC w 1989 r. Aktualne projekty norm uwzględniają uwagi zgłoszone do tych wersji.

Drugi z tych projektów [9], stanowi, że norma może być stosowana we wszystkich dziedzinach przemysłu, np. w przemysłach:

- **przetwórczym** (systemy wyłączania w przypadkach zagrożeń, sys-

[1] IEC – *International Electrotechnical Commission* (Międzynarodowa Komisja Elektrotechniczna) jest organizacją założoną w 1906 r., zajmującą się normalizacją międzynarodową w dziedzinie elektrotechniki.

[2] ISO – *International Organisation for Standardization* (Międzynarodowa Organizacja Normalizacyjna).

[3] *Programmable Electronic Systems in Safety-Related Applications: 1.An Introductory Guide, 2.General Technical Guidelines. HMSO, London, UK.*

[4] *Principles for Computers in Safety-Related Systems (Grundsatze für Rechner in System mit Sicherheitsaufgaben) DIN V VDE 0801, Beuth Verlag, Berlin, FRG (1990).*

[5] *Draft Standard Electrical Electronic Programmable Electronic Systems (PES) For Use in Safety Applications. Dostępny w: ISA Headquarters, PO Box 12277,67, Alexander Drive, Research Triangle Park, NC 27709, USA.*

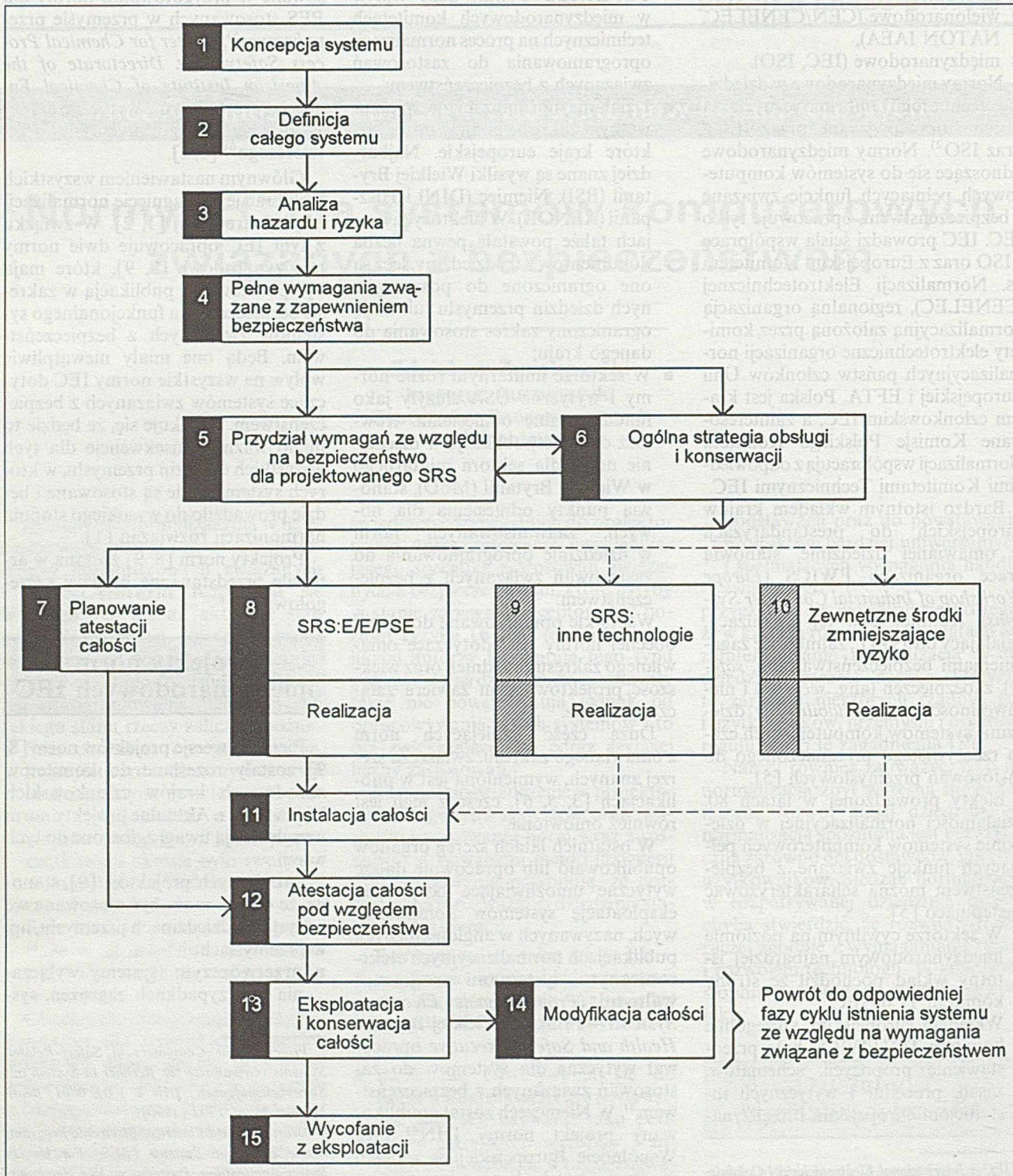
[6] *Guidelines for Safe Automation of Chemical Processes. Będzie opublikowany przez: The Center for Chemical Process Safety of the American Institution of Chemical Engineers, New York, NY 10017.*

temy detekcji ognia i gazu, kontrola palników),

- **wytwórczym** (roboty przemysłowe, obrabiarki),
- **aparatury medycznej** (różna aparatura medyczna, radiografia),
- **transporcie** (sygnalizacja kolejowa, systemy hamulcowe, dźwigi).

Niektóre podstawowe pojęcia stosowane w tej normie przedstawiono w [7].

W większości sytuacji bezpieczeństwo jest osiągane przez określoną licz-



Rys. 1. Cykl istnienia całego systemu ze względu na wymagania związane z bezpieczeństwem (ang. Overal Safety Lifecycle)

– SRS – Safety Related System (system związany z bezpieczeństwem), – E/E/PES – Electrical/Electronic/Programmable Electronic Systems (systemy elektryczne-elektroniczne-elektroniczne programowalne);

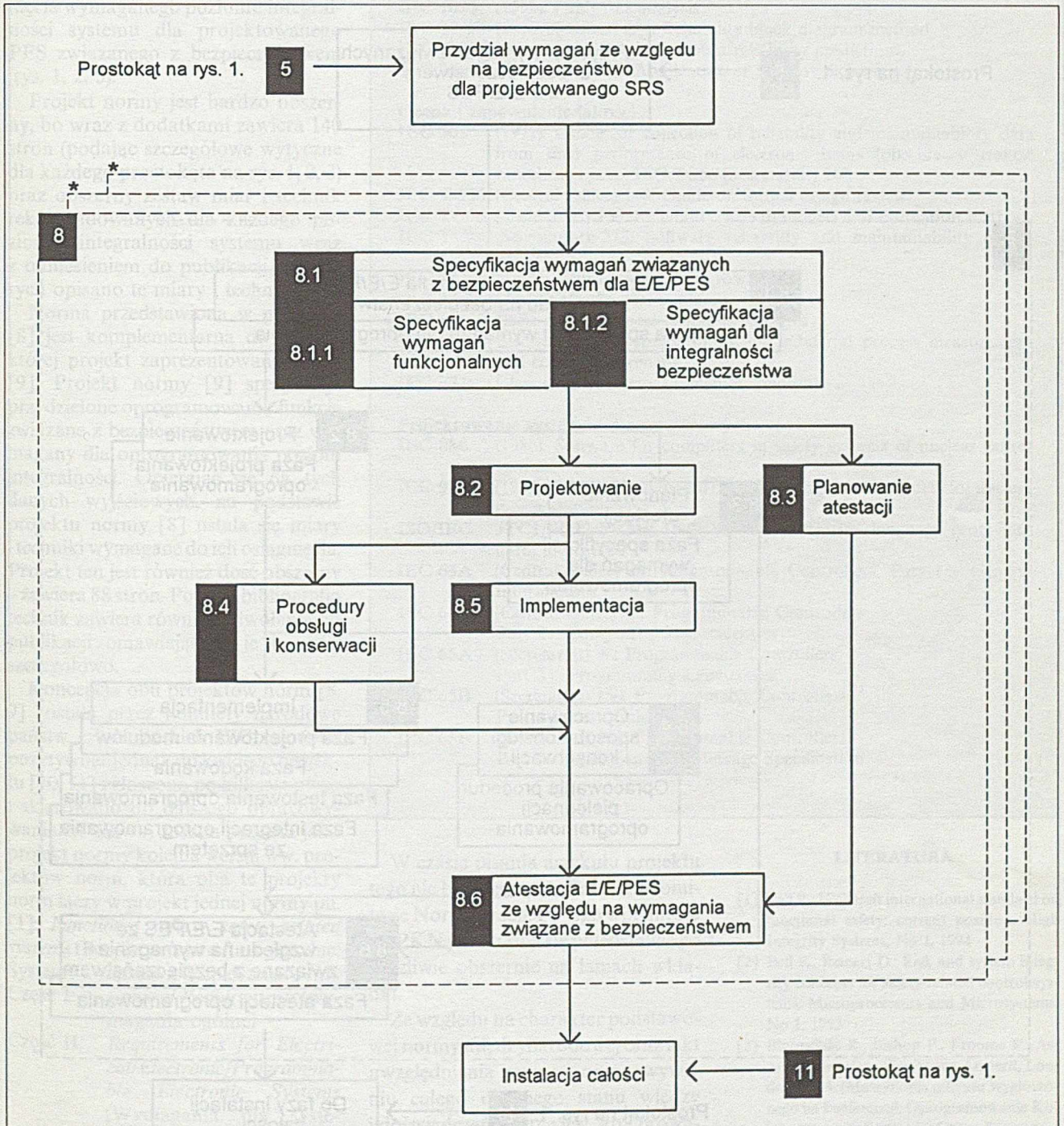
– Czynności *oceny* i *weryfikacji* nie są pokazane dla zachowania przejrzystości, ale są przewidziane dla wszystkich faz cyklu istnienia systemu;

– Czynności odnoszące się do faz przedstawionych w prostokątach 9 i 10 wyróżniono przez zakreskowanie dla wskazania, że norma nie zajmuje się w sposób szczegółowy tymi czynnościami

bę systemów zabezpieczających i opiera się na wielu technologiach (mechanicznej, hydraulicznej, pneumatycznej, elektrycznej, elektronicznej, programowalnej elektronicznej). Chociaż norma odnosi się głównie do systemów związanych z bezpieczeństwem złożonych urządzeń elektrycznych, elektronicznych lub programowalnych elektronicznych, to ma strukturę umożliwiającą jej zastosowanie do systemów związanych z bezpieczeństwem niezależnie od technologii, na jakiej są one oparte.

Przedstawiona w projekcie 9 norma opiera się na dwóch podstawowych koncepcjach:

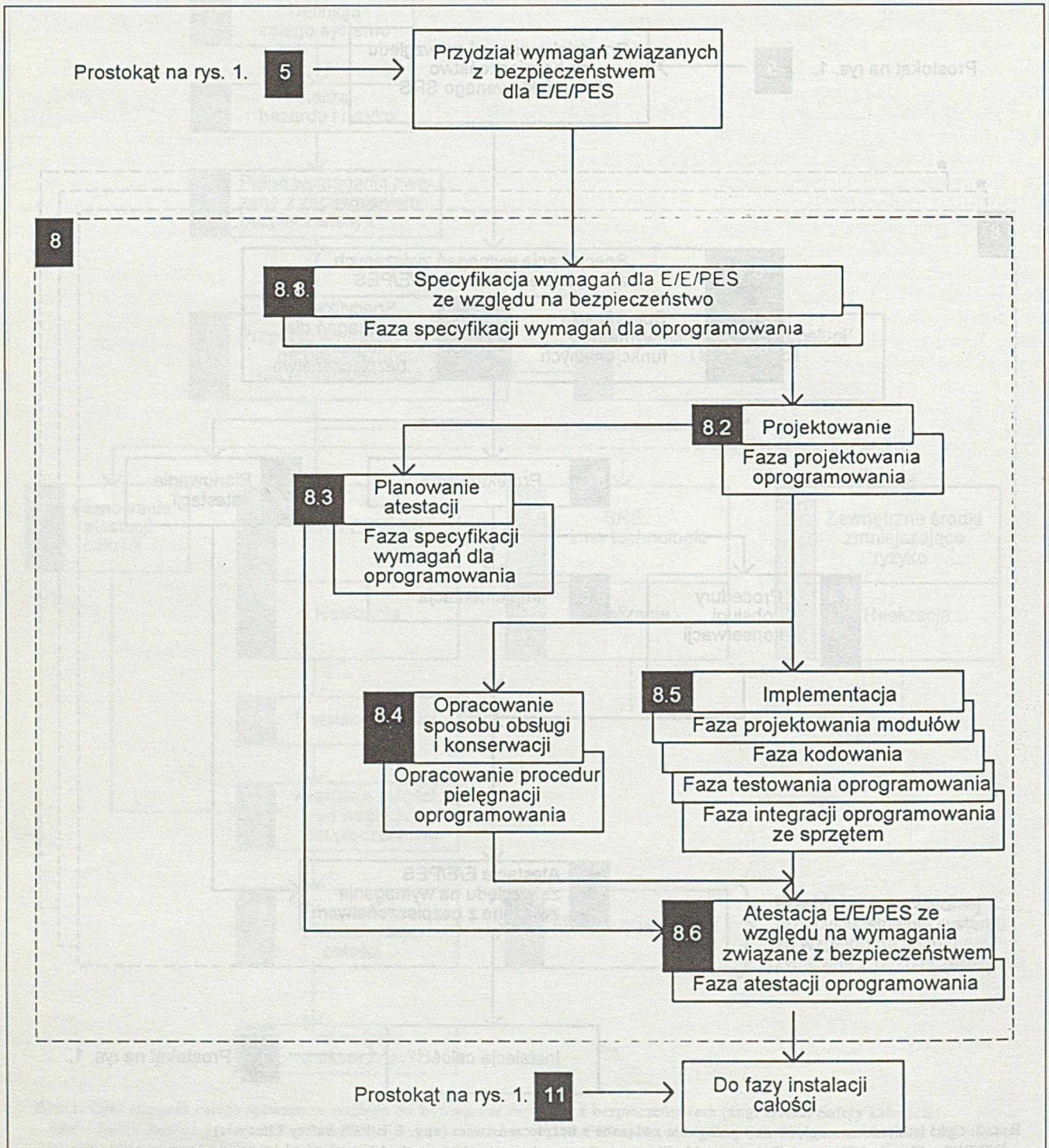
- wprowadzonej przez normę koncepcji Poziomów Integralności Systemu (ang. *System Integrity Levels*) w celu wyspecyfikowania wymaganego poziomu integralności bezpieczeństwa;
- modelu cyklu istnienia systemu ze względu na bezpieczeństwo (ang. *Safety Lifecycle*).



Rys. 2. Cykl istnienia ze względu na wymagania związane z bezpieczeństwem (ang. E/E/PES Safety Lifecycle)
- E/E/PES – Electrical/Electronic/Programmable Electronic Systems (systemy elektryczne-elektroniczne-elektroniczne programowalne);
- Przedstawiono procedury wymagane na 1 E/E/PES system związany z bezpieczeństwem;
- Czynności *oceny* i *weryfikacji* nie są pokazane dla zachowania przejrzystości, ale są przewidziane dla wszystkich faz cyklu istnienia E/E/PES związanego z bezpieczeństwem

Integralność bezpieczeństwa (ang. *Safety Integrity*) jest zdefiniowana w projekcie normy jako prawdopodobieństwo, że system związany z bezpieczeństwem będzie spełniał w określonym czasie wymagane funkcje związane z bezpieczeństwem w sposób satysfakcjonujący we wszystkich ustalonych warunkach. Projekt normy ustala cztery poziomy integralności i podaje sposoby za pomocą których, ustaliwszy tolerowalny poziom ryzyka dla danego systemu związanego z bezpieczeństwem, można ustalić wymagany poziom integralności systemu. Poziom ryzyka jest oceniany przez uwzględnianie zarówno konsekwencji, jak i częstotliwości przypadków hazardu [7].

W przypadku rozdzielenia funkcji związanych z zapewnieniem bezpieczeństwa na kilka systemów PES lub na PES oraz systemy zrealizowane z wykorzystaniem innych technologii (np. mechanicznej, hydraulicznej) oraz urządzenia zewnętrzne zmniejszające ryzyko, ustalenia wymaganego poziomu integralności systemu dla projek-



Rys. 3. Cykl istnienia E/E/PES ze względu na wymagania związane z bezpieczeństwem: odniesienia do cyklu istnienia oprogramowania (ang. E/E/PES Safety Lifecycle: Relationship to Software Lifecycle)
– E/E/PES – Electrical/Electronic/Programmable Electronic Systems (systemy elektryczne-elektroniczne-elektroniczne programowalne)

towanego PES dokonuje się po uwzględnieniu stopnia redukcji ryzyka, wnoszonej przez pozostałe ww. urządzenia pełniące również funkcje związane z bezpieczeństwem.

Przyjęty w projekcie normy model cyklu istnienia systemu ze względu na bezpieczeństwo umożliwia wykonanie w sposób usystematyzowany wszystkich czynności niezbędnych do osiągnięcia wymaganego poziomu integralności systemu dla projektowanego PES związanego z bezpieczeństwem (rys. 1, 2, 3).

Projekt normy jest bardzo obszerny, bo wraz z dodatkami zawiera 140 stron (podając szczegółowe wytyczne dla każdego prostokąta na rys. 1, 2, 3) oraz obszerny zestaw miar i technik rekomendowanych dla każdego poziomu integralności systemu wraz z odniesieniem do publikacji, w których opisano te miary i techniki.

Norma przedstawiona w projekcie [8] jest komplementarna do normy, której projekt zaprezentowano wyżej [9]. Projekt normy [9] specyfikuje przydzielone oprogramowaniu funkcje związane z bezpieczeństwem oraz wymagany dla oprogramowania poziom integralności. Opierając się na tych danych wyjściowych, na podstawie projektu normy [8] ustala się miary i techniki wymagane do ich osiągnięcia. Projekt ten jest również dość obszerny – zawiera 88 stron. Podana bibliografia technik zawiera również odwołania do publikacji omawiających je bardziej szczegółowo.

Koncepcja obu projektów norm [8, 9] została przez komitety narodowe państw członkowskich IEC oceniona pozytywnie, jednak do każdego projektu [10, 11] zgłoszono po kilkaset uwag i skierowano do dalszego opracowywania. W 1994 r. została przyjęta jako projekt normy kolejna wersja ww. projektów norm, która oba te projekty norm łączy w projekt jednej normy pn. [1]: *Functional safety: safety related systems* (Bezpieczeństwo funkcjonalne: Systemy związane z bezpieczeństwem).

Część I: *General Requirements* (wymagania ogólne)

Część II: *Requirements for Electrical/Electronic/Programmable Electronic Systems* (Wymagania dla systemów elektrycznych, elektronicznych, elektronicznych programowalnych)

Część III: *Software Requirements* (wymagania dla oprogramowania).

Wykaz istniejących norm oraz projektów norm dotyczących systemów komputerowych związanych z bezpieczeństwem

Analiza hazardu

IEC 812 (1985): Procedure for failure mode and effects analysis (FMEA)
IEC 1025 (1990): Fault tree analysis
IEC TC56 (Central Office) 137: Reliability block diagram method
IEC TC56 (Secretariat) 169: Parts count reliability prediction
IEC TC56 (Secretariat) 280: Application of Markov techniques

Ocena i zapewnienie jakości

IEC 362 (1971): Guide for collection of reliability and maintainability data from field performance of electronic items (obecnie w trakcie nowelizacji jako: IEC TC56 (Secretariat) 267
IEC TC56 (Central Office) 148: Guide on formal design review
IEC TC56 (Secretariat) 150: Reliability growth models and estimation methods
IEC TC56 (Secretariat) 273: Software reliability and maintainability management
IEC TC56 (draft) Software reliability growth
IEC TC56 (draft) Software test methods
IEC 68: Basic environmental testing procedures
IEC 801: Electromagnetic compatibility for industrial process measurement and control equipment
IEC 721: Classification of environmental conditions

Projektowanie systemów komputerowych

IEC 880 (1986): Software for computers in safety systems of nuclear power stations
IEC 987 (1989): Programmed digital computers important to safety for nuclear power stations
ISO/IEC JTC1/SC22/WG19 IN9: VDM specification language protostandard, draft, 1991
IEC 65A (Central Office) 21: Programmable Controllers, Part 1 – General Informations
IEC 65A (Central Office) 22: Programmable Controllers, Part 2 – Equipment Characteristics
IEC 65A (Secretariat) 90: Programmable Controllers, Part 3 – Programming Languagues
IEC 65B (Secretariat) 150: Programmable Controllers, Part 4 – User Guidelines
IEC 65B (Secretariat) 138: Programmable Controllers, Part 5 – Manufacturing Message Specification

W czasie pisania artykułu projektu tego nie było jeszcze w Polskim Komitecie Normalizacji. Po jego wpłynięciu do PKN postaramy się przedstawić go możliwie obszernie na łamach wkładki.

Ze względu na charakter podstawowej normy międzynarodowej oraz fakt uwzględnienia przy jej opracowywaniu całego obecnego stanu wiedzy i doświadczeń istotne jest, aby prowadzący lub planujący prace w tej dziedzinie w kraju możliwie wcześnie wiedzieli o przygotowywaniu takiej normy oraz znali jej koncepcję i projektowane postanowienia.

LITERATURA

[1] Bell R.: IEC draft international standard on functional safety: current position. High Integrity Systems, No 1, 1994
[2] Bell R., Reinert D.: Risk and system integrity concepts for safety-related control systems. Microprocessors and Microsystems, No 1, 1993
[3] Bloomfield R., Bishop P., Froome P.: Assuring the safety of software. Adelard, London, 1994. (Maszynopis referatu wygłoszonego na konferencji: Oprogramowanie Komputerowych Systemów Czasu Rzeczywistego, Wrocław, 22–23.09.1994)
[4] Fuji R., Guerdat C., Sullo P.: International software engineering standards: facing the challenge. Fourth Software Engineering

dokończenie na s. 32

Windows NT w energetyce.

Systemy i aplikacje Microsoft to nie tylko pakiety, oprogramowanie, podręczniki i licencje. To przede wszystkim konkretne zastosowania i wygoda użytkowania. W poprzednich numerach Informatyki opisywaliśmy już system operacyjny Microsoft Windows NT, teraz pokażemy, w jaki sposób stosują go nasi sąsiedzi za miedzą, w bardzo ważnym obszarze gospodarki - w energetyce.

EZ Inc. zajmuje się produkcją i przesyłaniem energii elektrycznej. Centrum Dyspozycyjne przedsiębiorstwa jest odpowiedzialne za zarządzanie systemem energetycznym Republiki Czeskiej i z tego względu współpracuje także z kooperantami zagranicznymi. Wiąże się to ze zbieraniem i przetwarzaniem **w czasie rzeczywistym** danych telemetrycznych z ponad stu miejsc na terenie całego kraju (kluczowe to elektrownie i podstacje przesyłowe).

Dane są gromadzone, wstępnie przetwarzane i poddawane obróbce statystycznej, a ich wyniki są podstawą do podejmowania decyzji n.t. wykorzystania bloków energetycznych w elektrowniach. Rejestrowana jest także obciążalność sieci energetycznej i dystrybucja energii, co stanowi podstawę do obliczeń zużycia energii, jak i przewidywania możliwych spiętrzeń i problemów.

Warunki początkowe

Pierwotnie system dyspozycyjny zbierał dane z sieci energetycznej i przetwarzał je, używając dużych maszyn IBM serii 4341, 4361 i komputerów Comparex. Używano systemu OS/V1 i VM/DS z bazą danych SQL.

Cały system wymagał wykonania 1800 pomiarów i zarejestrowania 2200 sygnałów w ciągu minuty. Dodatkowo, oprócz pomiarów wykonywane były periodyczne i nieperiodyczne obliczenia.

Nowe podejście

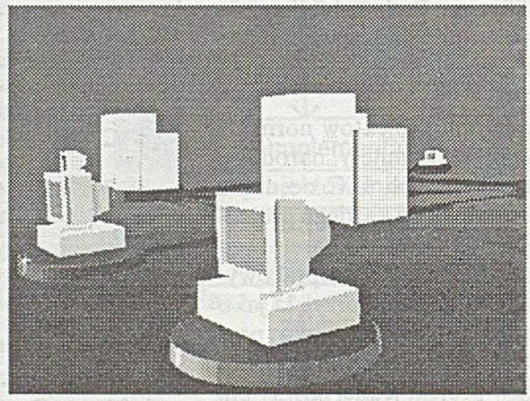
W 1991 podjęto decyzje o zbudowaniu systemu opartego o sieci LAN/WAN i użyciu rozproszonej bazy danych. Do pierwszego etapu realizacji wyznaczono dwie filie w Pradze:, oraz jedną w Ostrawie. Podstawowym celem tego etapu realizacji było uzyskanie dostępu do odpowiedniej informacji w ramach sieci LAN/WAN z dowolnego stanowiska roboczego. W 1994 roku sieć komputerowa miała trzy domeny, a cały system oparty był o serwery wyposażone w Windows NT 3.1 Advanced Server. Dane operacyjne zbierane z sieci gromadzone były w bazie danych Microsoft SQL Server 4.2, pracującej pod systemem Windows NT Advanced Server..

Ze względu na zapewnienie absolutnego bezpieczeństwa wszystkie serwery baz danych zostały zdublowane. Wszystkie aplikacje decyzyjne zostały dokładnie przetestowane, tak że nie zaobserwowano przerw w pracy systemu w przypadku wystąpienia awarii.

Połączenia pomiędzy filiami w Pradze realizowane są przez radiolinie Telettra o przepustowości 2 Mbit/s i w najbliższej przyszłości zostaną najprawdopodobniej zastąpione przez światłowody.

Back-up danych jest realizowany przez łącze 9.6 kbit/s. Połączenie logiczne zapewnia most. Pomiędzy Pragą i Ostrawą wykorzystano łącze X.25 o przepustowości 64 kbit/s i routery.

Microsoft SQL Server 4.2 użyto nie tylko do obsługi bazy danych, ale także do okresowych obliczeń statystycznych i inżynierskich, jak np. obliczenia przewidywanych wartości parametrów sieci energetycznej, topologii sieci, oraz optymalizacji użycia generatorów.



Zalety rozwiązania

W porównaniu z systemem wykorzystującym komputery mainframe zaobserwowano wzrost wydajności pracy oraz skrócenie czasu przetwarzania - na niektórych odcinkach ponad 100 razy!

Niezawodnosc pracy systemu jest również dużą zaletą. Wprowadzenie graficznego środowiska Microsoft Windows jest dużą zaletą, przetwarzanie danych na stanowiskach roboczych staje się dużo łatwiejsze.

0/12/95

Mobitex już w Warszawie

System bezprzewodowej transmisji danych wkracza do Polski

W Warszawie powstała pilotowa instalacja do radiowej transmisji danych w systemie Mobitex. System jest stosowany do przesyłania danych w ruchu oraz wszędzie tam, gdzie jest niezbędny błyskawiczny dostęp do informacji, bez oczekiwania na połączenie. Terminale w pojazdach policji (kartoteki), samochodach dostawczych (zarządzanie taborem), w drobnych sklepach i bankomatach (weryfikacja kart kredytowych) – to jedynie niektóre z możliwych zastosowań Mobitexu. Ogólnie chodzi tu o kluczowe dane o niewielkiej objętości. Mobitex działa już w Austrii, Finlandii, Francji, Holandii, Norwegii, Szwecji, Wielkiej Brytanii, Kanadzie i USA.

W polskim przedsięwzięciu uczestniczy Ericsson Polska jako dostawca technologii, TELBANK SA jako operator systemu oraz Mobitel – inwestor i dystrybutor radiomodemów do sieci Mobitex. Operatorzy Mobitexu spodziewają się początkowo zainteresowania ze strony firm, które już wcześniej korzystały z usług tej sieci w innych krajach, np. DHL czy Coca-Cola. Z czasem urośnie także i grono rdzennych klientów. Najprawdopodobniej potężnym użytkownikiem będzie system bankowy. Z doświadczenia wynika, iż opłacalne jest inwestowanie w system już przy 200–300 pojedynczych użytkownikach.

Cennik obejmuje dzierżawę modemów (150–230 zł mies.), opłaty instalacyjne (60–800 zł), rozmaite abonamenty (80–1240 zł) oraz opłaty za ruch. Te ostatnie liczone są za liczbę przesłanej informacji i wahają się od 1 do 4 groszy za 0.1 kB w zależności od liczby danych i pory dnia. Ceny mogą się zdawać wygórowane, ale należy pamiętać, że przy większości zastosowań Mobitexu obracamy danymi rzędu kilku bajtów, co w efekcie przynosi oszczędności nawet w porównaniu z połączeniem telefonicznym. Cykl zwrotu kosztów inwestycji wynosić ma dla użytkownika komercyjnego zaledwie od kilku do kilkunastu miesięcy.

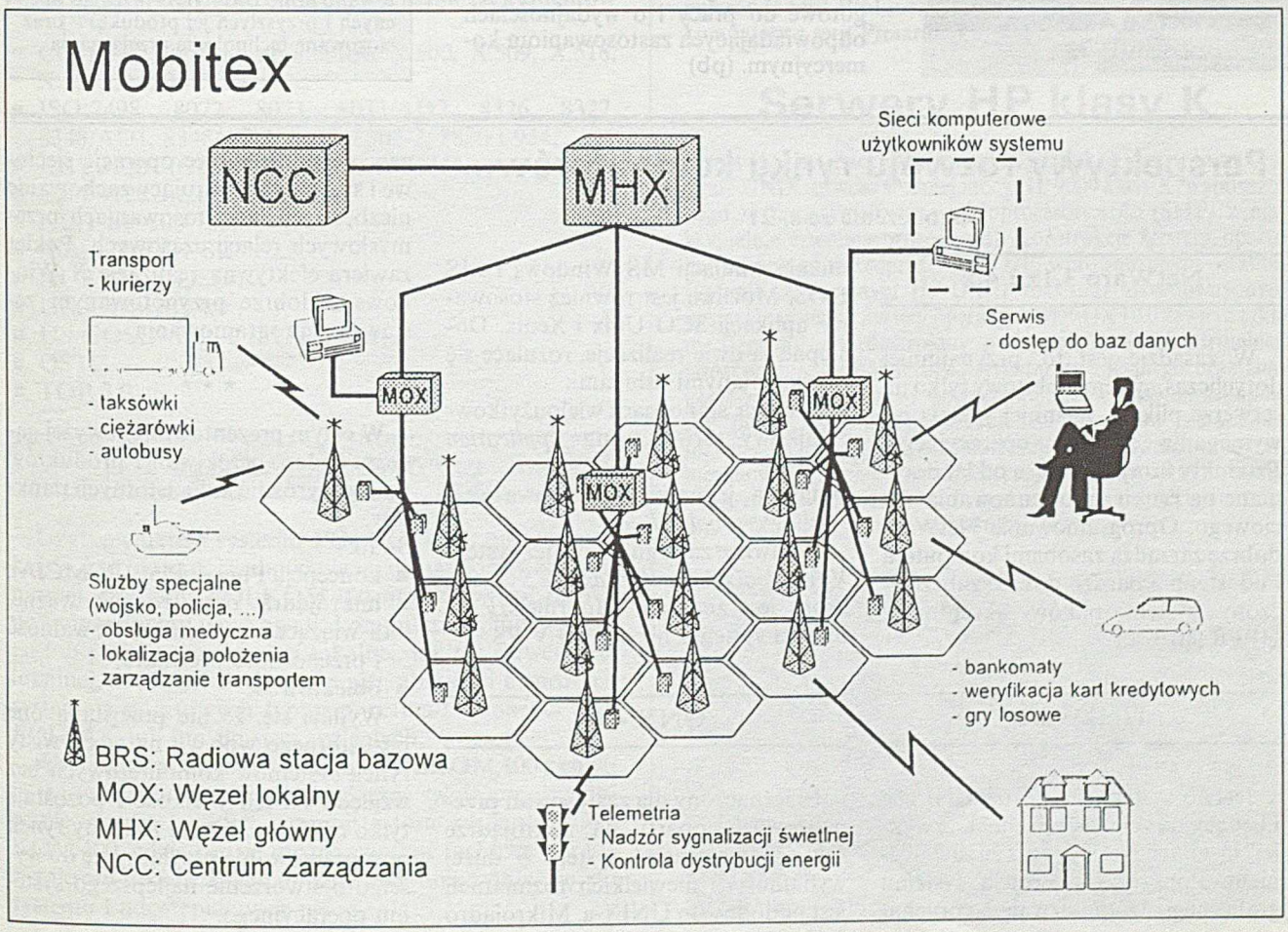
Pod względem technicznym Mobitex jest systemem o komutacji pakietów, co pozwala, tak jak Internet, na pozorną jednoczesność wszystkich połączeń. Sieć danego kraju składa się z centrum zarządzania, węzła głównego i węzłów lokalnych. Do tych ostatnich podłączone są radiowe stacje bazowe o zagęszczeniu odpowiednim dla zapewnienia całkowitego pokrycia danego terenu łącznością. Użytkownik ze swoim systemem macierzystym ma dostęp do któregoś z węzłów lokalnych, najczęściej za pomocą dedykowanych łączy przewodowych. Dane wędrują w przewodowej części Mobitexu a następnie, od stacji bazowych, drogą radiową do urządzeń z radiomodemami.

Ponieważ Mobitex stanowi jedynie medium do transmisji pakietów danych, rodzaj urządzenia końcowego i oprogramowania może być dowolny, byle dało się do niego podłączyć radiomodem (RS323C, PCMCIA i in.). Wymiana danych odbywa się automatycznie zawsze ze stacją najlepiej słyszalną. Sieci Mobitex na świecie projektowane są tak, by docelowo pokryć swoim zasięgiem 95% populacji danego kraju.

U nas, jak dotychczas, objęta jest nią Warszawa, w której znajduje się sieć pilotowa z czterema stacjami bazowymi. Do końca roku ma zostać włączonych do Mobitexu pięć największych miast Polski. Sieci w poszczególnych państwach docelowo stanowić mają jednolity system. Operatorów Mobitexu zrzesza MOA (*Mobitex Operator's Association*). Mobitex ma bramki do innych sieci, m.in. do Internetu, jednak ze względu na nieduże prędkości transmisji ok. 8000 b/s i duże opłaty za objętość danych, zastosowanie ogranicza się głównie do ograniczonej wymiany poczty i baz danych. Aplikacje do użytku w sieci Mobitex są optymalizowane pod kątem maksymalnego ograniczenia zbędnych informacji oraz kompresji.

Mobitex nie usiłuje współzawodniczyć z innymi sieciami. Ma on zastosowanie tam, gdzie potrzebna jest szybka wymiana danych bez oczekiwań na połączenie z miejscami, użycie specjalizowanych połączeń przewodowych byłoby nieekonomiczne, oraz do systemów mobilnych. Potencjalny rynek na tego typu usługi, jak oceniają firmy związane z tworzeniem systemu, jest w Polsce olbrzymi.

Przemysław Baszkiewicz



WebForce – pakiet komercyjnej obsługi WWW

Firma Silicon Graphics Industries przedstawiła w Warszawie na seminarium zorganizowanym przy współudziale swojego dystrybutora na terenie Polski – firmy ATM, nową linię oprogramowania i komputerów pod nazwą WebForce. WebForce jest specjalistycznym zestawem środków do tworzenia, przeglądania i obsługi systemu World Wide Web.

Od strony sprzętowej oferta dzieli się na zestawy uniwersalne, będące równocześnie stacjami autorskimi i serwerami, oraz na oddzielne systemy specjalnego przeznaczenia. Komputery SGI znane są powszechnie z zastosowań multimedialnych, a ich efektywność w WWW zapewnić mają konfiguracje oparte na mikroprocesorach MIPS R4600, szynach systemowych 267 MB, 32 MB pamięci RAM oraz obszernym wyborze łączy sieciowych. Ceny zaczynają się od ok. 15 tys. USD. Do zestawów autorskich SGI dołącza programy Adobe Photoshop, Adobe Ilustrator oraz enkoder MPEG. Jest też WebMagic – edytor HTML 2.0 pracujący w konwencji WYSIWYG.

WebMagic jest łatwy w obsłudze i pozwala bezboleśnie wykorzystywać pliki graficzne, filmowe i dźwiękowe. WebMagic nie zaskakuje nowością rozwiązań, ale w zestawieniu z szybkim komputerem i poręcznym pakietem aplikacji multimedialnych jest z pewnością jednym z lepszych narzędzi dostępnych na rynku. Maszyny pracujące w roli serwerów wyposażono w oprogramowanie firmy Netscape Communications: do wyboru Netsite Communications Server lub Netsite Commerce Server. Pierwszy z programów ma zastosowanie w reklamie i porozumiewaniu się z klientami, drugi pozwala na dokonywanie bezpiecznych zakupów i transakcji w sieci. Konfiguracje serwerów zaprojektowano tak, aby mogły wytrzymać duże zainteresowanie internautów.

Według SGI konfiguracja podstawowa wraz z oprogramowaniem Netscape może obsłużyć dziennie nawet 150 tys. zamówień na dokumenty. Oferta SGI jest przeznaczona głównie dla firm obsługujących duże systemy WWW. Cena jest wysoka, jak na nasze warunki, ale w zamian za to użytkownik dostaje bogate zestawy, całkowicie gotowe do pracy i o wydajnościach odpowiadających zastosowaniom komercyjnym. **(pb)**

Zaprosili nas ...

Polska Izba Informatyki i Telekomunikacji wraz ze Stowarzyszeniem Oficjalnych Importerów Samochodów i Stowarzyszeniem Producentów Kosmetyków i Chemii Gospodarczej na wspólną konferencję, w trakcie której przedstawili uchybienia formalno-prawne związane z dotychczasową procedurą certyfikacji produktów, prowadzoną przez Polskie Centrum Badań i Certyfikacji. Zaproponowali zawieszenie na okres dwóch lat obowiązku uzyskiwania certyfikatów, co pozwoli obu stronom – jednostce certyfikującej i przedstawiającej produkt do certyfikacji na dopasowanie swoich procedur postępowania.

Multitrade SA i firma Novell Polska Sp. z o.o. do szkoły komputerowej na spotkanie inaugurujące działalność Autoryzowanego Centrum Szkoleniowego Novella (NAEC). Na spotkaniu zaprezentowano polską wersję produktu GroupWise oraz omówiono aktualną ofertę i perspektywy szkoleń w zakresie produktów Novella.

Apple Computer IMC Poland, Sad Ltd. na konferencję połączoną z przedpremierowym pokazem najnowszego multimedialnego komputera Macintosh Performa 5200 CD. Przedstawiono strategię działania firmy w zakresie promocji produktów na przykładzie komputera Macintosh LC 630 oraz zaprezentowano najnowsze czasopismo o Macintosh-ach – Macword.

POLIXEL S.A. na seminarium pt. „Przełączanie i gładkie przejście na ATM", organizowane przez firmę LANNET i jej partnerów. Zaprezentowano firmę LANNET, przegląd obecnych i przyszłych jej produktów oraz stosowane technologie przełączania.

Perspektywy rozwoju rynku komputerów...

dokończenie ze s. 21

NetWare 3.1x i 4.x

W zasadzie jest to, przynajmniej dotychczas, system 32-bitowy tylko na serwerze plików, niemniej spełnia on wymagania systemu operacyjnego. Produkty firmy Novell są od lat doceniane na rynku oprogramowania sieciowego. Oprogramowanie NetWare dobrze zarządza zasobami komputera i udostępnia bardzo dobrze zabezpieczony system plików akceptujący HPFS lub FAT.

UnixWare

Jest to system oparty na UNIX-ie i będący raczej uzupełnieniem „zwykłej" instalacji NetWare niż jej zastąpieniem. Poprawna realizacja systemu graficznego *Motif* pozwala na uruchamianie emulacji MS Windows i MS DOS. Możliwe jest również stosowanie aplikacji SCO Unix i Xenix. Dostępne są dwie realizacje, różniące się udostępnianymi usługami:

- droższa, stanowiąca wieloużytkownikowy serwer usług *Application Server*,
- tańsza, jednoużytkownikowa wersja *Personal Edition*.

Na uwagę zasługuje również system VxFS (*UnixWare Veritas File System*), który jest znacznie odporniejszy na upadki systemu niż system V FS.

QNX 4.0

Przeznaczony dla zastosowań przemysłowych, oparty na mikrojądrze QNX MicroKernel system o dużej wydajności i niewielkich rozmiarach jest podobny do UNIX-a. Mikrojądro zawiera podstawowe operacje sieciowe i system gwarantujący zachowanie niezbędnych w zastosowaniach przemysłowych relacji czasowych. Pakiet zawiera efektywną realizację X Windows z dobrze przygotowanym zestawem oprogramowania.

* * *

W całym prezentowanym wyżej gąszczu żądań, oczekiwań i produktów należy wyróżnić kilka istotnych punktów.

Są to:

- koncepcja Plug & Play (PCMCIA),
- mikrojądra oraz równie ważne, a wiążące się z nimi skalowalność i przenośność produktu,
- obiektowość

Wydaje się, że nie pozostaną one bez istotnego wpływu na rzeczywisty rynek systemów komputerowych bez względu na ich wielkość i pozostaje tylko mieć nadzieję, że rodzimy rynek oprogramowania przyłączy się do wyścigu o stworzenie najlepszego systemu operacyjnego.

3Com – zarządzanie pakietami w środowisku SNA/IBM

3Com proponuje nowe urządzenia sieciowe, które pośredniczą w przekazywaniu pakietów między lokalną a rozległą siecią komputerową. Nowy system zarządzania pakietami jest przeznaczony dla zdalnych połączeń biur terenowych w sieciach SNA (*System Network Architecture*), charakterystycznych dla środowiska sieci komputerowych IBM. Do tego celu przeznaczony jest *router* 3COM serii NETBuilder Remote Office, który będzie sprzedawany z wyposażeniem optymalizującym wyznaczanie trasy pakietu dla struktury SNA. Dodatkowo 3Com dostarcza oprogramowanie do zarządzania siecią – *Transcend Network Management* – przeznaczone dla sieci SNA.

3Com wprowadził całą rodzinę produktów zwiększających wydajność pracy w miejscu łączenia się sieci ze sobą. *Smart Filters* (filtry inteligentne) redukują natężenie ruchu pakietów w przypadku stosowania dwóch różnych protokołów transmisji SNA oraz NetBIOS, minimalizując w ten sposób niepotrzebny ruch pakietów w sieci. *Payload compression* – dzięki kompresji metodą „payload" pakiet jest skompresowany z ramki o długości 200 bajtów, do ramki o długości 50 bajtów. Zastosowanie algorytmu kompresji powoduje czterokrotne skrócenie długości pakietu, a więc i czasu transmisji.

Automatic prioritization – zastosowanie automatycznego wyboru kolejności przesyłania pakietów – pozwala na zachowanie przywileju pierwszeństwa dla pakietów SNA przed innymi protokołami transmisji. Opcja *Local termination* eliminuje konieczność powtórnego logowania się w przypadku powstania przerw w transmisji. (k)

Koncepcja realizacji poczty elektronicznej ...

dokończenie ze s. 11

- CCITT X.435 Elektroniczna Wymiana Dokumentów – EDI,
- CCITT X.500 Spis abonentów X.500, X.509, X.518, X.519, X.520 i X.521,
- ISO 7498, 8072, 8073, 8073/AD2, 8326, 8327, 8348/AD1, 8348/AD2, 8473, 8802-2, 8880 i 9542,
- ENV 41201 (CEN/CENELEC A/3211),
- ENV 41202 (CEPT A/311),
- NIST SP 500-183,
- Australian GOSIP v.2.0,
- NORDIC GOSIP,
- UK GOSIP v.4.0 i 4.1,
- US GOSIP v.1 i 2 (FIPS 146-1),
- OSTC,
- TOP 3.0

Użytkownicy systemu

Użytkownikiem systemu POLKOM 400 może zostać każdy, kto ma zapotrzebowanie na usługi poczty elektronicznej. Z systemu POLKOM 400 może korzystać zarówno indywidualny użytkownik komputera wolno stojącego lub pracującego w sieci lokalnej, jak też serwer sieci lokalnej, abonenci sieci teleksowej, abonenci firmowych systemów pocztowych typu np. cc:mail, abonenci sieci POLPAK lub innych sieci rozległych.

Aby zostać abonentem systemu POLKOM 400 z chwilą jego uruchomienia należy zgłaszać swoje zapotrzebowanie do CST-TPSA, administratora systemu POLKOM 400, gdzie będzie można uzyskać fachową poradę z zakresu technicznych możliwości dołączania się do systemu i udostępnianych usług.

Compaq Presario – więcej niż komputer

Nową linię mutimedialnych komputerów Presario – 700, 900 i CD TV 528 – zaprezentował Compaq w auli Akademii Sztuk Pięknych w Warszawie (maj br.). Wszystkie mają napędy CD-ROM poczwórnej prędkości, stereofoniczną kartę dźwiękową, procesory DX2/66 i DX4 klasy 586, z możliwością rozbudowy. Presario może zastąpić telefon, ma bowiem wbudowany mikrofon, co umożliwia prowadzenie rozmów bez podnoszenia widocznej na ekranie słuchawki. Jest też wyposażony w sekretarkę automatyczną, faks-modem i notes telefoniczny, umożliwiający automatyczne wybieranie numerów. Należący do serii Presario – CD TV 528 pozwala oglądać audycje telewizyjne, obrazy wideo na ekranie monitora i odbierać telewizję kablową. Zapewnia to wielostandardowy tuner TV. Wystarczy do komputera podłączyć anteną telewizyjną lub kabel telewizji kablowej, a otrzymujemy swoisty kombajn wieloczynnościowy. Komputery Presario wyposażone są w oryginalne oprogramowanie Media Pilot, które z punktu widzenia użytkownika jest graficznym symulatorem pilota stosowanego do obsługi telewizora czy innych urządzeń audiowizualnych. Użytkownik uruchamia poszczególne funkcje multimedialne wybierając poszczególne przyciski na ekranie Presario. Obraz telewizyjny można oglądać w wydzielonym oknie, korzystając równocześnie z innych aplikacji, lub powiększyć na cały ekran.

Wprowadzenie na rynek nowych modeli Presario zbiegło się w czasie z ogłoszeniem obniżki cen, nawet o 12%, na niektóre komputery z poprzedniej serii Presario. I tak Presario CDS 744 kosztuje 1599 USD (obniżka o 100 USD), a cena Presario CDS 982 spadła z 2499 USD do 2199 USD. Compaq może sobie na to pozwolić; sprzedaż w I kwartale br. w stosunku do analogicznego okresu ub.r. wzrosła o 30%, zysk firmy w I kwartale br. wyniósł 216 mln USD (o trzy miliony więcej niż w I kwartale 1994 r.). Strategia firmy polega na nieustannym atakowaniu rynku nowościami. W pierwszej połowie tego roku Compaq zaoferował m.in. ponad 100 nowych modeli komputerów z serii ProLinea, dwa typy serwerów i opisane wyżej komputery z serii Presario. (k)

Serwery HP klasy K

Firma Hewlett-Packard rozpoczęła produkcję opartego na systemie UNIX serwera średniej mocy HP 9000 klasy K, wyposażonego w tzw. symetryczną wieloprocesorowość (SMP) z maksymalnie czterema procesorami. Konstrukcję serwera oparto na technologii mikroprocesorów HP, wprowadzonym ostatnio systemie operacyjnym HP-UX(1) 10.0 oraz zrównoważonym projekcie systemu. System operacyjny HP-UX 10.0 zawiera takie mechanizmy, jak dostrojony podsystem pamięci wirtualnej, udoskonaloną współbieżność systemu operacyjnego oraz znaczące zwiększenie liczby operacji wejścia–wyjścia na sekundę. HP poleca swój nowy produkt szczególnie do zastosowań inżynierskich, w tym do automatyzacji projektowania urządzeń mechanicznych i elektronicznych, projektowania oprogramowania, systemów informacyjnych, rynków ropy naftowej i gazu oraz architektury, inżynierii i konstrukcji. (k)

Normy IEC dla systemów komputerowych związanych z bezpieczeństwem

dokończenie ze s. 27

Standards Application Workshop, May 20–24, 1991, San Diego, California. Proceedings edited by IEEE computer Society Press, Los Alamitos, 1991

[5] Gonzales Sanz J.: Standardization for safety software: current status and perspectives. Fourth Software Engineering Standards Application Workshop, May 20–24, 1991, San Diego, California. Proceedings edited by IEEE computer Society Press, Los Alamitos, 1991

[6] Wright C.L., Zawilski A.J.: Existing and emerging standards for software safety. Fourth Software Engineering Standards Application Workshop, May 20–24, 1991, San Diego, California. Proceedings edited by IEEE computer Society Press. Los Alamitos, 1991

[7] Żurakowski Z.: Systemy komputerowe w zastosowaniach związanych z bezpieczeństwem. Informatyka, nr 3, 1995

[8] IEC Draft 65A (Secretariat) 122 (1991): Software for computers in the application of industrial safety-related systems

[9] IED Draft 65A (Secretariat) 123 (1992): Functional safety of electrical /electronic/ programmable electronic systems. Generic aspects. Part 1: General requirements

[10] IEC 65A (Secretariat) 146 (1993): Resulting of voting on Commitee Draft 65A (Secretariat) 122

[11] IEC 65A (Secretariat) 147 (1993): Compilation of comments on Commitee Draft 65A (Secretariat) 123.

Bylicki A.: Bezpieczeństwo systemów informatycznych
INFORMATYKA 1995, nr 7, s. 1
Szczegółowe omówienie rozwiązań gwarantujących logiczne bezpieczeństwo wewnętrzne unixowych systemów komputerowych.

Michalski S., Suskiewicz M.: Koncepcja realizacji poczty elektronicznej X.400 w TP S.A.
INFORMATYKA 1995, nr 7, s. 8
Charakterystyka rozwiązań wprowadzanej w Polsce przez TP S.A. poczty elektronicznej POLKOM 400, opartej na standardzie X.400.

Abt S.: Systemy logistyczne wyzwaniem dla informatyków
INFORMATYKA 1995, nr 7, s. 12
Zadania i funkcje informatyki w projektowaniu i realizacji współczesnych systemów logistycznych.

Szyjewski Z.: Homologacja systemów informatycznych
INFORMATYKA 1995, nr 7, s. 16
Uzasadnienie potrzeby oraz propozycja rozwiązań organizacyjnych dla wprowadzenia procedury homologacji systemów informatycznych.

Repeć R.: Perspektywy rozwoju rynku komputerów osobistych
INFORMATYKA 1995, nr 7, s. 19
Charakterystyka aktualnych trendów rozwoju sprzętu oraz systemów operacyjnych komputerów osobistych.

Żurakowski Z.: Normy IEC dla systemów komputerowych związanych z bezpieczeństwem
INFORMATYKA 1995, nr 7, s. 22
Charakterystyka międzynarodowej działalności normalizacyjnej oraz projektów norm IEC, przeznaczonych dla systemów komputerowych związanych z bezpieczeństwem działania.

Bylicki A.: Data processing systems security
INFORMATYKA 1995, No. 7, p. 1
Detailed discussion of solutions, which warrant internal logic security of the unix computer systems.

Michalski S., Suskiewicz M.: Idea of the X.400 e-mail realization in the TP S.A.
INFORMATYKA 1995, No. 7, p. 8
Charakteristics of solutions for the POLKOM 400 e-mail, which is introduced in Poland by the Polish Telecommunication Inc. (TP S.A.) and is based on the X.400 standard.

Abt S.: Logistic systems as a challenge for IT specialists
INFORMATYKA 1995, No. 7, p. 12
Data processing tasks and functions in designing and realization of contemporary logistic systems.

Szyjewski Z.: Data processing systems homologation
INFORMATYKA 1995, No. 7, p. 16
Necessity reasons and proposal of organizational solutions for introducing of data processing system homologation.

Repeć R.: Development prospects of the PC market
INFORMATYKA 1995, No. 7, p. 19
Characteristic of actual development trends in hardware and operating systems of personal computers.

Żurakowski Z.: IEC standards for safety related computer systems
INFORMATYKA 1995, No. 7, p. 22
Characteristics of international standardization activity and of the IEC standard drafts for safety related computer systems.

Bylicki A.: Die Sicherheit von EDV-Systemen
INFORMATYKA 1995, Nr. 7, S. 1
Detaillierte Besprechung von Lösungen, die eine innere logische Sicherheit der unixartigen Computersysteme garantieren.

Michalski S., Suskiewicz M.: Eine Konzeption für Realisierung von X.400 elektronischer Post im TP S.A.
INFORMATYKA 1995, Nr. 7, S. 8
Eine Charakteristik von Lösungen der vom Polnischen Telekommunikation AG (TP S.A.) eingeführten POLKOM 400 elektronischen Post, die auf dem X.400-Standard gestützt wurde.

Abt S.: Logistische Systeme als Herausforderung für Informatiker
INFORMATYKA 1995, Nr. 7, S. 12
EDV-Aufgaben und -Funktionen bei Projektierung und Realisierung von zeitgenössischen logistischen Systemen.

Szyjewski Z.: Die Homologation von EDV-Systemen
INFORMATYKA 1995, Nr. 7, S. 16
Notwendigkeitsbegründung und ein Vorschlag der organisatorischen Lösungen für Einführung der Homologationsprozedur von EDV-Systemen.

Repeć R.: Entwicklungsaussichten des PC-Marktes
INFORMATYKA 1995, Nr. 7, S. 19
Eine Charakteristik von heutigen Entwicklungstendenzen im Bereich der Hardware und Betriebssysteme von Personalcomputern.

Żurakowski Z.: Die IEC-Normen für Sicherheitscomputer-systeme
INFORMATYKA 1995, Nr. 7, S. 22
Eine Charakteristik von der internationalen Normungstätigkeit und von den IEC-Normenprojekten für Sicherheitscomputersysteme.

Pierwsza kolorowa igłowa drukarka Oki

Firma Oki rozpoczęła produkcję kolorowej drukarki atramentowej – OKIJET 300c. Drukarka ma wbudowaną emulację języka PCL 3, która jest rozszerzeniem zbioru poleceń drukarki HP DeskJet 500c, obsługującym pisma o zmiennym stopniu. Zainstalowane ma trzy kroje pism zmiennej wielkości (od 4 do 128 punktów) oraz dwa kroje rastrowe PCL. Można też ładować czcionki do pamięci RAM drukarki. OKIJET 300c jest wyposażona w zmienne głowice drukujące do kolorów i pojedynczej barwy. Magazynek na papier mieści 140 arkuszy. Drukarka pracuje z różnymi rodzajami i formatami papieru, drukuje też na folii. Szybkość druku – 3 strony na minutę, rozdzielczość druku – 300 × 300 dpi. Wyposażona jest w standardową pamięć 21 KB.

Matrix-UPS – modułowy zasilacz

Zasilacz awaryjny serii Matrix-UPS wykonany w technice line-interactive to oferta firmy American Power Conversion dla dużych systemów komputerowych typu midrange. W środowiskach typu klient/serwer Matrix-UPS współpracując z oprogramowaniem PowerChute 4.x zapewnia kontrolę wszystkich serwerów pracujących w sieci z możliwością wydania poleceń wyłączenia „zagrożonych" komputerów. Matrix składa się z dwóch modułów: wyposażenia elektronicznego oraz izolacyjnego zawierającego transformator. Zastosowano transformator izolujący galwanicznie elementy elektroniczne zasilacza, co stanowi dodatkową ochronę przed skutkami zwarcia. Matrix wyposażony został w układ do automatycznej regulacji napięcia wyjścia sterowany mikroprocesorem Fine-Line. Zasilacze dostępne są w dwóch wersjach: Matrix 3000 o mocy 2250 W i Matrix 5000 o mocy 3750.

Znachor – program dla lekarzy

Znachor 7.2 – to program firmy Pablo przeznaczony dla lekarzy i służący do wprowadzania, przechowywania oraz statystycznego opracowywania danych. Jego podstawową zaletą jest funkcja, umożliwiająca statystyczne przetwarzanie danych o pacjentach i gromadzenie tych danych na czytelnie rysowanych, standardowych w służbie zdrowia arkuszach. Informacje można wprowadzać do programu w czasie rozmowy z pacjentem, nie można natomiast – zgodnie z wymaganiami Ministerstwa Zdrowia – wstecznie korygować wyników badań. To sprawia, że dane są wiarygodnym źródłem informacji, możliwym do wykorzystania nawet w sądzie. Program ma skromne wymagania sprzętowe: PC 286, dowolna karta graficzna, 640 KB pamięci operacyjnej. Firma Pablo gwarantuje też łatwość dołączania aparatu ekg, eeg oraz przesyłania danych przez modem. Znachor może działać również w sieci.

Compaq ProLiant 1500 z zegarem 120 MHz

Compaq podjął produkcję nowego serwera Compaq ProLiant 1500 5/120, który jest wyposażony w procesor Pentium 120 MHz Intela. Serwer został tak zaprojektowany, by zapewnić użytkownikom dostęp do mechanizmów zarezerwowanych dawniej tylko dla największych i najdroższych komputerów tej klasy, takich jak Compaq ProLiant 2000 i Compaq ProLiant 4000, a jest konkurencyjny cenowo wobec nich (ok. 10 700 USD). Klienci Compaqa, którzy już mają serwer ProLiant 1500, mogą dokonać upgrade'u za pomocą karty z Pentium 120 MHz. Standardowo maszyna jest dostarczana z 32-bitowym sterownikiem Fast-Wide SMART SCSI-2-EISA lub PCI oraz dwoma dyskami twardymi Fast-Wide SCSI-2 o pojemności 2,1 GB. Ponadto serwer jest wyposażony w pamięć ECC, architekturę systemową TriFlex/PCI oraz obsługę Fast-Wide SCSI-2, ASR-2, napędy i macierze dyskowe podłączone w trakcie prac systemu oraz zdublowane zasilacze sieciowe. Procesor systemowy w ProLiant 1500 5/120 można będzie wymienić na szybsze procesory lub płyty procesorów Intela, gdy tylko będą one dostępne na rynku.

Sterownik Fibre Channel z HP

Pierwszy na rynku sterownik Fibre Channel-Tachyon, zintegrowany do postaci pojedynczego układu scalonego, wprowadziła na rynek firma Hewlett-Packard. Zaprojektowano go z myślą o superszybkich zastosowaniach w podłączonych do sieci urządzeniach pamięci masowej. Umożliwia on przesyłanie danych z szybkością rzędu gigabajtów na sekundę (dane przesyłane przez kanały światłowodowe z prędkością do 100 MB/s). Tachyon pozwoli producentom urządzeń pamięci masowej na znaczne skrócenie cyklu projektowego oraz obniżkę kosztów produkcji, związanych do tej pory z rozwiązaniami wymagającymi bardzo dużych prędkości transmisji. Już ponad 40 firm z całego świata wyraziło zainteresowanie Tachyonem i włączyło układ do nowo projektowanych produktów. Jako pierwsze powstaną produkty zapewniające połączenie komputerów głównych z superszybkimi urządzeniami pamięci masowej, takimi jak stacje dysków, tablice pamięciowe oraz jednostki archiwizujące dane na taśmie. Układ jest tani, co zapewne przyśpieszy rozwój technologii Fibre Channel.

LANDesk Management Suite 2.0 Intela

Firma Intel zaprezentowała pierwszy zintegrowany pakiet do zarządzania siecią lokalną – LANDesk Management Suite 2.0. Jest on nie tylko zbiorem narzędzi, pozwalających wykonać konkretne operacje, ale dostarcza administratorowi gotowych rozwiązań problemów, z jakimi najczęściej ma on do czynienia w czasie pracy, oraz zapewnia mu pełną kontrolę nad sposobem funkcjonowania sieci. Pakiet Intela ma wydajne mechanizmy wymiany i gromadzenia informacji, takie jak system raportowania przebiegu pracy sieci, system alarmowania w razie wystąpienia nieprawidłowości oraz możliwość wymiany informacji z innymi aplikacjami. LANDesk Management Suite 2.0 ma zaimplantowany standard OLE, potrafi też komunikować się z innymi popularnymi systemami do zarządzania siecią. Zawiera też oddzielny, pracujący w standardzie OLE moduł, który pozwala użytkownikowi tworzyć własne aplikacje łączące w jedną całość funkcje różnych narzędzi.

AutoCAD OEM dla projektantów

Autodesk przygotował dla programistów nowy produkt z rodziny AutoCAD – AutoCAD OEM. Będzie on dostępny dla projektantów, którzy przystąpią do ogłoszonego jednocześnie programu Autodesk OEM.

Równocześnie firma oferuje OEM Component Technologies – zestaw wyspecjalizowanych modułów, które pozwalają włączyć do tworzonych aplikacji technologie związane z modelowaniem, animacją, rysunkiem lub renderingiem. Każdy z modułów podlega osobnej licencji, co umożliwia dostosowanie zakupu do konkretnych wymagań stawianych przed aplikacją. W skład Autodesk OEM Component Technologies wchodzą: AutoCAD OEM – środowisko programistyczne umożliwiające korzystanie z AutoCAD Application Programing Interfaces; HOOPS – narzędzie graficzne, które pozwala stosować we własnych aplikacjach interakcyjną grafikę 3D; AutoVision OEM – narzędzie gwarantujące generowanie w aplikacji wysokiej jakości obrazu metodą renderingu; Cyberspace Developers Kit (CDK) – narzędzie programistyczne umożliwiające tworzenie interakcyjnych modeli rzeczywistości wirtualnej i ich komunikację z produktami Autodesku z dziedziny multimediów i CAD; ADE OEM (AutoCAD Data Extension) umożliwiające tworzenie połączeń między danymi w formacie AutoCAD, a innymi bazami danych.

Opracowała:
Krystyna Karwicka-Rychlewicz

Perfect-Ekspert

AITECH

20 LAT DOŚWIADCZEŃ WDROŻENIOWYCH

Wysoka jakość

Wysoka jakość

„Polifarb" Cieszyn S.A.
Zakłady Rowerowe „ROMET"
Krywald „ERG" S.A.
Elektrownia Rybnik Huta Łaziska
Fabryka Osi Napędowych - Radomsko
Zakłady Tłuszczowe „BIELMAR"
Elektromontaż 3 Huta Bankowa
Zakłady Metalurgiczne „Trzebinia"
Walcownia Metali „Dziedzice" Huta Szkła „Kunice"
POLAM Kostuchna Zakłady Gumowe Górnictwa
Huta 1-go Maja

IBM PC IBM PC IBM PC IBM PC

ODRA 1305

AS/400 AS/400 AS/400

AS/400

1995

Zakres funkcjonalny

Sieciowy i zintegrowany system informatyczny, głównie dla dużych firm produkcyjnych i handlowych. Przystosowany do elektronicznej wymiany dokumentów (EDI - zamówienia, faktury, WZ, itp.), wielowalutowości, denominacji złotego oraz rachunkowości zarządczej. Wyposażony w system ochrony danych generowanych wewnątrz i na zewnątrz przedsiębiorstwa. Współpracujący z systemem ekspertowym ISAF (Inteligentny System Analiz Finansowych) wspomagający **podejmowanie decyzji finansowych na średnich i wyższych szczeblach zarządzania.**

ADVELL

System Informacji Kierownictwa	Inteligentny System Analiz Finansowych	System Finansowo-Kosztowy	System Wyposażenie
System Obrotu Towarowego i Fakturowania	System Obrotu Materiałami i Ewidencji Zakupu	Rozliczenie Zakupu Materiałów	System Środki Trwałe
System Kadry - Płace	System Analiz Marketingowych	System Technicznego Przygotowania Planowania i Rozliczania Produkcji	EDI TMW Ultra - Perfect

1987

Zakres funkcjonalny

Oferujemy kompleksowe usługi w zakresie:
- doradztwa organizacyjnego, merytorycznego, technicznego, consulting,
- organizacji, projektowania i wykonawstwa innych systemów informatycznych,
- wdrażania, konserwacji i modernizacji systemów informatycznych,
- projektowania, wykonawstwa dowolnego typu sieci komputerowych, z uwzględnieniem już istniejących rozwiązań,
- dostawa sprzętu komputerowego i sieciowego,
- szkoleń użytkowników w zakresie operatora i administratora systemu AS/400, jak również obsługi pakietów programowych PC Support/400 lub Client Access/400 przeznaczonych do współpracy z PC.

JUNISOFTEX

44-100 Gliwice, ul. Kościuszki 1 c, box 507
Tel./fax (0-32) 31-51-31, 31-57-00
38-80-52, 38-80-54

JUNISOFTEX